2009-12

Deterring terrorism a framework for making retaliatory threats credible

Tippet, Douglas F.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DETERRING TERRORISM: A FRAMEWORK FOR MAKING RETALIATORY THREATS CREDIBLE

by

Major Douglas F. Tippet

December 2009

Thesis Advisor:	Jeffrey W. Knopf
Second Reader:	Zachary S. Davis

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Deterring Terrorism: A Framework for Making Retaliatory Threats Credible		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Major Douglas F. Tippet			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

To deter terrorism, U.S. deterrence strategy must threaten retaliatory responses that are appropriate to the actions by non-state actors the United States wishes to prevent. The effectiveness of those threats depends on the perceived credibility that America possesses the capability and willingness to execute them. Although U.S. policy focuses on preventive and preemptive counterterrorism strategies, this thesis argues that it contains relevant targets for retaliation but lacks credibility because its threats do not distinguish between types of attack. Instead of correlating threats to undesirable actions, it declares the same punishment for all terrorism, which is unrealistic ex post. On the contrary, the level of response should be proportionally related to the type and destructive effects of an attack and in tune with the level of public outrage the attack would generate.

This thesis first provides theoretical support for the claim that recent U.S. policy documents contain valid threats for influencing non-state actors. Then, credibility is evaluated by comparing those threats to the expected U.S. response for two dissimilar scenarios: cyber and nuclear terrorism. The analysis suggests that policy threats lack credibility because the signaled response for terrorism holds constant across varying degrees of attack severity. Because the likely responses to these attacks differ in practice, the undifferentiated signals sent by recent policy weaken deterrence. As a result, the thesis recommends establishing a retaliation framework based on type of attack.

14. SUBJECT TERMS deterrence, terrorist attack, non-state actor, retaliation, retribution, punitive deterrence, deterring terrorism, reprisal, nuclear terrorism, cyber terrorism, terrorist vulnerabilities, terrorism			**15. NUMBER OF PAGES** 108
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DETERRING TERRORISM: A FRAMEWORK FOR MAKING RETALIATORY THREATS CREDIBLE

Douglas F. Tippet
Major, United States Air Force
B.S.M.E., University of Arkansas, 1995

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2009**

Author: Douglas F. Tippet

Approved by: Jeffrey W. Knopf
Thesis Advisor

Zachary S. Davis
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To deter terrorism, U.S. deterrence strategy must threaten retaliatory responses that are appropriate to the actions by non-state actors the United States wishes to prevent. The effectiveness of those threats depends on the perceived credibility that America possesses the capability and willingness to execute them. Although U.S. policy focuses on preventive and preemptive counterterrorism strategies, this thesis argues that it contains relevant targets for retaliation but lacks credibility because its threats do not distinguish between types of attack. Instead of correlating threats to undesirable actions, it declares the same punishment for all terrorism, which is unrealistic ex post. On the contrary, the level of response should be proportionally related to the type and destructive effects of an attack and in tune with the level of public outrage the attack would generate.

This thesis first provides theoretical support for the claim that recent U.S. policy documents contain valid threats for influencing non-state actors. Then, credibility is evaluated by comparing those threats to the expected U.S. response for two dissimilar scenarios: cyber and nuclear terrorism. The analysis suggests that policy threats lack credibility because the signaled response for terrorism holds constant across varying degrees of attack severity. Because the likely responses to these attacks differ in practice, the undifferentiated signals sent by recent policy weaken deterrence. As a result, the thesis recommends establishing a retaliation framework based on type of attack.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to thank God for my loving family who provided me with their enduring support not only during this endeavor to accomplish a Master's degree but also through the many trials of our military service. To my amazing wife, Jennifer, son, Jordan, daughters, Madison and Lauren; thank you for your encouragement when I struggled and your understanding during those times I was unavailable.

Also, my humble gratitude goes out to Professor Jeff Knopf for his guidance and expertise in the field of deterrence which enabled me to complete this project. And, finally, I would like to thank the Naval Postgraduate School faculty and staff for a world-class education that greatly expanded my knowledge base and really challenged me to think on a higher level.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

While many actions have been taken to better secure the U.S. homeland from catastrophic terrorist attacks, one strategy potentially underutilized is deterrence. In recent years, Homeland Security doctrine has relied heavily on two defensive strategies: disrupting operations and protecting critical targets. Although both remain relevant and necessary to counter terrorism, they have inherent limitations that make it advisable to consider supplementing these strategies with a more robust deterrence policy. Lewis Dunn describes the recent policy like this:

> For the most part, however, recent attention has focused on consequence management, and to a lesser extent prevention of incidents involving nuclear, chemical, or biological weapons. Deterring terrorist or sub-national use has been essentially dismissed out of hand. This may be faulty logic.[1]

First, prevention is extremely difficult and unlikely to be foolproof. To discern actual plans in the malevolent rhetoric of elusive organizations, and then manage to disrupt, capture, and punish offenders before they actually commit the act, is an enormous undertaking. This arduous task not only puts a tremendous burden on agencies tasked with uncovering the covert plans of veiled organizations, but forces them to perform a balancing act between maintaining security and upholding civil liberties. Second, as difficult as it is to prevent an attack, the goal of making the citizens and infrastructure of the United States impenetrable is practically impossible. Elbridge Colby claims that "in between these two extremes, deterrence is a security policy that offers a way forward for the United States that is not only more effective because more tailored, but is also more moral."2 Therefore, an effective deterrence by punishment policy should play a critical role in a comprehensive counterterrorism strategy.

---

[1] Lewis A. Dunn, "Rethinking Deterrence: A New Logic to Meet Twenty First Century Challenges" In *Deterrence and Nuclear Proliferation in the Twenty-First Century*, ed. Stephen J. Cimbala, (Westport, Conn.: Praeger, 2001), 23–38, 24.

[2] Elbridge Colby, "Restoring Deterrence," *Orbis* 51, no. 3 (Summer, 2007), 413–428, 424.

This thesis explores the characteristics of a retribution policy that would support a Homeland Security strategy aimed at deterring non-state actors from attacking the United States. It claims that, to improve the deterrent effect of counterterrorism strategies, the United States should tailor threats of punishment to match the crime (the latter based roughly on the magnitude of harm) because this approach will increase the credibility of its deterrent message. To support this claim, the study examines the declared threats of punishment for terrorist attacks that are found in recent policy, and evaluates whether those responses would be politically acceptable whilst having the desired effect. It is important to note that for the purpose of this study the objective is to deter terrorist attacks on the United States, not to deter the existence of terrorism itself.

B. PURPOSE

One way that the United States signals deterrence is through its national strategy documents and, more specifically, the threats of punishment contained therein. The effectiveness of these threats depends on the perceived credibility that the United States possesses the capability and willingness to execute them. Assuming the United States has the capability, the effectiveness of deterrence is dependent upon the credibility of the retaliatory threat. Although U.S. policy shifted after September 11, 2001 (9/11) towards preemptive and preventive methods to strike targets of terrorism, I argue that: 1) it also contains relevant deterrent threats that 2) lack credibility because there is no distinction between types of attack and threatened response. To clarify the second point, it is the public declaration of current policy that I scrutinize, not whether policy makers understand how to prescribe realistic responses for different attacks. The reason for this focus is that public declaratory policy is one of the most visible ways in which the United States communicates deterrent threats to non-state actors.

With this in mind, I intend to qualitatively analyze the various threats of retaliation through a scenario-based evaluation to show that U.S. policy lacks deterrence credibility, and suggest that a deterrence framework that links retaliatory threats to the type of terrorist attack would solve this problem. The objective of this thesis is first to validate that counterterrorism policies of the United States contain relevant threats of

punishment for effective deterrence, and then analyze these threats as potential forms of punishment in response to different attack scenarios, thereby showing that credibility of those threats is degraded when they are not correlated to the type of attack.

The thesis closes by suggesting that U.S. deterrence strategy should contain an attack-based framework for retaliation in order to credibly threaten violent non-state actors and advocating continued development of punitive deterrence methods for Homeland Security. If credible threats were identified for each type of terrorist attack, then the United States could institutionalize the appropriate responses into a clearly articulated deterrence policy. Developing a retaliation framework, based on type of attack, provides a critical step in bridging the gap between theories on deterring terrorism and current counterterrorism strategies, to form a more relevant and effective policy for deterring terrorism.

C. REQUIREMENTS OF EFFECTIVE DETERRENCE

Deterrence, as it relates to national security strategy, can be divided into two categories. First, state deterrence addresses threats to national security from both nuclear and conventional acts of war committed by other nations. Strategies for implementing this type of deterrence are relatively straightforward in policy and widely accepted due to the tangibility of punishing states. The second category, however, strives to deter domestic and transnational actors from attempting random acts of violence that inflict property damage and injury to citizens. Punishment threats for this type of deterrence are found in the U.S. penal codes for prosecuting domestic terrorists and U.S. national strategy documents for non-state actors.

Setting aside domestic criminology, the debate on whether punitive deterrence is an effective strategy to deter non-state actors mainly concentrates on the question of credible retaliation. To be more concise, what practical form of retaliation would deter terrorists from committing attacks? In contemplating this question, it is apparent that terrorist organizations do not fit into the traditional framework for deterring states. Although some of the established standards for state deterrence are applicable to non-

state actors, those of retribution are mostly inapplicable. And while retribution remains a critical component of deterrence, defining a retaliation policy for counterterrorism presents unique challenges. Therefore, several approaches to deterring non-state actors are rooted in traditional theories of criminology, because terrorists' behavioral patterns emulate those of criminal organizations that operate either within or outside the national boundaries.[3] Nevertheless, an effective deterrence strategy should incorporate a policy that describes the behavior to be deterred, and the retaliation it will invoke, if committed.

In order to effectively deter a violent non-state actor, there must be a potential to influence its decision cycle. This would presume that non-state actors follow some process to evaluate options and predict outcomes when making decisions. The ability to influence these decisions is important because deterrence by punishment necessitates that something of value can be held at risk, which would only hold true if non-state actors calculate expected utility. The difficulty rests in identifying, and then plausibly threatening, targets of significance to the terrorists. While a state fears loss of material power, public support and sovereignty, terrorists are non-state actors that may be able to operate without geographical or demographical constraints. Therefore, deterring terrorist attacks comes down to identifying what terrorists covet and fear, then transforming that into a credible threat message. However, any threat that trespasses the boundaries of American sense of justice or breaks international norms would not be credible forms of retaliation. Consequently, identifying significant targets to threaten with credible means and intent is a complicated, although necessary, task.

D. LITERATURE REVIEW

The origins of deterrence theory are traced to studies of crime and punishment by Jeremy Bentham, who postulated that criminals rationally consider punishment costs when deciding whether to commit a crime. He further stated that having clear, consistent, and proportional punishment provides a certain level of predictability that

[3] Ariel Merari, "Deterring Fear: Government Responses to Terrorist Attacks," *Harvard International Review* 23, no. 4 (Winter, 2002), 26–31, 26.

enhances deterrence effects.[4] During the Cold War, scholarly research went through phases that were creatively described by Jervis as the "three waves" of deterrence theory.[5] However, the bipolar system that was so central in these strategies dissolved with the end of the Cold War, ushering in a new era of asymmetric threats. Jeffrey Knopf describes this new phase as the "fourth wave" of deterrence research, which focuses on deterring non-state actors and rogue regimes through both denial and punishment methods.[6] A significant amount of the current literature debates the usefulness and practicality of deterrence as an effective strategy for U.S. policy in a unipolar system faced with asymmetric threats.

Although some negate its efficacy, most experts agree that deterrence remains a viable strategy against asymmetric threats. The literature can be subdivided into two general categories based on the underlying assumption of whether a state can possibly deter non-state actors (terrorist organizations). On one side of the argument, researchers presume terrorists are irrational fanatics that cannot be deterred and, therefore, suggest indirect deterrence strategies aimed at rogue states and those providing support that enables terrorist attacks. Paul Kapur proposes a "third-party" punishment strategy to deter entities that provide finances, weapons, asylum, and other support to terrorists, instead of attempting to target irrational, elusive terrorists themselves.[7] A significant amount of literature in this category runs parallel to counter-proliferation objectives, in the sense that it seeks to influence the supply-side of WMD transfer. David Auerswald suggests that preventing WMD transfer remains the most important goal, and posits a denial and punishment strategy aimed at transnational criminal organizations that might engage in trafficking WMD materials.[8] On the contrary, Elbridge Colby argues that

---

[4] Lawrence Freedman, *Deterrence* (Cambridge, UK : Malden, MA: Polity Press, 2004), 145, 8.

[5] Lawrence Freedman, *Deterrence* (Cambridge, UK : Malden, MA: Polity Press, 2004), 145, 21.

[6] Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research" (forthcoming in *Contemporary Security Policy*).

[7] S. Paul Kapur, "Deterring Nuclear Terrorists" In *Complex Deterrence: Strategy in the Global Age*, eds. T. V. Paul, Patrick M. Morgan and James J. Wirtz (Chicago: London: The University of Chicago Press, 2009), 117.

[8] David P. Auerswald, "Deterring Nonstate WMD Attacks," *Political Science Quarterly* 121, no. 4 (Winter, 2006), 543–568, 567.

WMD proliferation is inevitable and trying to prevent it is a waste of resources; therefore, deterring attacks by threatening those who enable terrorism remains the preeminent strategy that, if effective, would reduce the incentive for acquiring WMD.[9] Alexander George provides three forms of indirect deterrence that seek to influence state sponsorship by enlisting third-party influence, bolstering one side of a divided leadership, or applying pressure from an opposing regime.[10] Melese and Angelis move beyond state-based deterrence to suggest a United Nations deterrence strategy to discourage terrorists from acquiring and using WMD under the threat that the Secretary General would react to WMD activities by ceasing efforts to restrain Security Council members from preemptive or retaliatory strikes.[11] In summary, these studies explore the employment of denial and punishment strategies to prevent non-state actors and rogue states from providing terrorists with safe-havens, weapons, materials, or technology.[12]

The second category of literature suggests that although a few committed martyrs behave irrationally, other members of the organization logically calculate the cost-to-benefit ratio of their decisions.[13] Although there remains some skepticism as to what degree, this literature supports direct deterrence approaches that also suggest both denial and punishment strategies. For example, Trager and Zagorcheva suggest using deterrence by denial and punishment against all components of the terrorist system, focusing on their political aims especially when dealing with local issues.[14] Nonetheless, the majority of work here focuses on denial methods, mainly due to the difficulty

---

9 Colby, "Restoring Deterrence," 413–428, 427.

10 Alexander L. George, "The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries" In *Know Thy Enemy: Profiles of Adversary Leaders and their Strategic Cultures*, eds. Barry R. Schneider and Jerrold M. Post, 2nd ed. (Maxwell Air Force Base, AL: Wash. D.C.: USAF Counterproliferation Center, 2003), 325, 275.

11 Francois Melese and Diana Angelis, "Deterring Terrorists from using WMD: A Brinkmanship Strategy for the United Nations," *Defense & Security Analysis* 20, no. 4 (Dec, 2004), 337–341, 339.

12 Wyn Bowen, "Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism," *Contemporary Security Policy* 25, no. 1 (2004), 54–70., 67; Kapur, *Deterring Nuclear Terrorists*, 122.

13 Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism: It can be done," *International Security* 30, no. 3 (Winter, 2005), 87–123, 88; Bowen, *Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism*, 54–70, 62.

14Trager and Zagorcheva, "Deterring Terrorism: It can be done," 87–123, 99.

associated with applying punishment strategies to non-state actors. These studies propose a defensive strategy, in which deterrence by denial is achieved by protecting targets to increase the relative cost of perpetrating attacks while marginalizing their potential effects in an effort to dissuade terrorists.[15] Amid this debate, few discard a punishment strategy but suggest rather a policy that utilizes both while describing the potential of denial methods with greater emphasis.[16]

The main argument against this defensive approach points out that it is impossible to protect everything and while terrorists may be deterred from attacking a hardened target, this deterrence effect does not preclude them from exploiting a soft target instead.[17] Furthermore, a nation has infinite vulnerabilities, so attempting to secure all of them would be an ineffective use of resources that, in the end, could prove economically disastrous.[18] When considering these limitations, evidence suggests that deterring terrorist attacks by threat of punishment provides a logical supplement to the aforementioned strategies, not only because it helps fill the gaps left by the impractical task of securing a limitless number of targets or disrupting covert operations, but also because it deals with the inevitability of proliferation. For example, deterring rogue states from supporting terrorism seems realistic when the U.S. possesses ultimate military superiority, but what credible threat could it impose on Russia for nuclear proliferation violations (intentional or inadvertent)—certainly not nuclear retaliation. On the other hand, effectively deterring terrorists from committing catastrophic attacks eliminates the demand for WMD and, therefore, removes the predicament of punishing Russia or any other world power for allowing WMD to leak to non-state actors.

---

[15]Trager and Zagorcheva, "Deterring Terrorism: It can be done," 87–123, 91.

[16]Bowen, "Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism," 54–70, 67; Cimbala, *Deterrence and Nuclear Proliferation in the Twenty-First Century*, 185, 170.

[17]Bowen, “Deterrence and Asymmetry,” 62.

[18] Elbridge A. Colby, "Expanded Deterrence: Broadening the Threat of Retaliation," *Policy Review*, no. 149 (Jun/Jul, 2008), 43–59, 44; Paul K. Davis and Brian M. Jenkins, *Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda* (Santa Monica, CA: Rand, 2002), 86, http://www.rand.org/publications/MR/MR1619/ (accessed 4/15/2009), xiv.

However, in assuming that a more holistic policy should include strategies for deterring terrorist organizations by threat of punishment, the practicality of a plausible retaliation remains. Successful deterrence by punishment hinges on the premise that the deterrer can clearly communicate a credible threat of severe retaliation against a terrorist group's center of gravity if they attack. Literature on this topic discusses methods to overcome the complications associated with first identifying terrorist vulnerabilities, next determining how to legitimately retaliate, and then effectively communicating a deterrent message. The major research dealing with directly influencing terrorist organizations comes from Davis and Jenkins. They hypothesize that, while a few fanatics may be irrational, a large number of members in a terrorist system—leaders, lieutenants, religious figures, logistical elements and recruiters—can be influenced.[19] Arguments claiming that terrorists cannot be deterred seem to focus on the suicidal foot soldiers and overlook other important members of the organization.[20] For example, during the Cold War, the objective of deterrence was not to deter individual soldiers of the Soviet military, but to convince leaders and key elements that launching an attack would prove detrimental to their goals and livelihood. Therefore, identifying the vulnerabilities or desires of other amenable members of the group would provide objectives for credible retaliation that when explicitly communicated, or executed after an attack, would conceivably lead to an effective deterrent. Many proponents suggest that the U.S. response to the attacks by al Qaeda on September 11, 2001 has provided a foundation for deterrence by punishment from which to build a solid policy.[21] Lawrence Freedman hence concludes that "the claim that deterrence does not work with terrorism can be challenged … [because] even if some attacks succeed, little political consequence will follow and those responsible can expect that they will be hounded down and punished."[22]

Again, a fundamental component of building a credible retribution is that the punisher can target something of value to the deterree. Trager and Zagorcheva, for

[19]Colby, "Expanded Deterrence: Broadening the Threat of Retaliation," 43–59, xi.

[20]Ibid., xii.

[21]Ibid., 47.

[22]Freedman, *Deterrence*, 145, 124.

example, recommend targeting the entire terrorist system and groups' political goals with retaliatory threats.[23] Additionally, Gerald Steinberg and others suggest that retribution should incorporate massive retaliation, even excessive in proportion, to increase the terrorists' realized costs beyond acceptable levels.[24] Colby calls for an expanded deterrence strategy that would not only threaten retaliation against those operationally involved, but to everyone involved including governments and entities that cooperate or are complicit with an attack.[25] Daniel Whiteneck discusses threatening "interests of society," such as striking public infrastructure, but warns that attacks on other supporting infrastructure like schools, religious centers, or civilians would do more harm than good.[26] He states, the "key is to extend deterrence using conventional and nuclear forces to the societal elements that support terrorism."[27] Although these target-restriction arguments remain valid, they are based on the assumption that retaliation means military strikes; but, as Knopf points out, broader "fourth wave" research increasingly explores non-military options when proposing acceptable forms of retribution.[28] Threatening these targets would not necessarily invoke military retaliation, but would utilize other elements of national power to produce the desired influence.[29]

Finally, an effective deterrence policy must include a deterrent message so the deterree undoubtedly comprehends the consequences of specific actions. As Whiteneck puts it, "to make the deterrent threat clearer and to maximize its credibility, an adversary must be able to predict soundly what the scope of a state's response to an attack could be, not just what it would be."[30] The message must convey the relationship between the

---

[23]Trager and Zagorcheva, "Deterring Terrorism: It can be done," 87–123, 88.

[24]Gerald M. Steinberg, "Rediscovering Deterrence After September 11, 2001," *Jerusalem Letter/Viewpoints* No. 467 (2001), http://www.jcpa.org/jl/vp467.htm (accessed 4/10/2008).

[25]Colby, "Expanded Deterrence: Broadening the Threat of Retaliation," 43–59, 46.

[26]Daniel Whiteneck, "Deterring Terrorists: Thoughts on a Framework," *The Washington Quarterly* 28, no. 3 (Summer, 2005), 187–199, 194–195.

[27]Ibid., 198.

[28]Knopf, "The Fourth Wave in Deterrence Research," 18.

[29]Davis and Jenkins, "Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda," 86, xiii.

[30]Whiteneck, "Deterring Terrorists: Thoughts on a Framework," 187–199, 189.

important elements of action and reaction, and will be even more effective if the reaction has some level of automaticity. Several authors describe a strategy that would punish those who cross clearly-articulated red lines like attacks using nuclear, biological or chemical weapons (NBC).[31] However, as Knopf accurately points out, the use of chemical or biological agents does not always equate to a weapon of mass destruction.[32] Therefore, it is important to define specifically the retaliatory response based on the level of damage, not just the type of weapon employed in an attack. Hence, accurately defining the type of attack that constitutes a violation (red line crossed) and its correlated retaliation could provide the basis for an effective deterrent strategy. Lastly, it is important to institutionalize the retaliatory response to make it nearly automatic, thereby removing any doubt on the part of terrorists that "bureaucratic deliberation" would interfere.[33] Auerswald emphatically states that, "Most importantly, our deterrence threats stand a better chance of appearing credible if we demonstrate that we have no choice but to implement our threats should that be necessary."[34]

In closing, regardless of what methodology the literature employed, the majority of reviewed research positively advocated the value of deterrence strategy in preventing terrorism. Also common throughout this research, experts acknowledged the limitation of deterrence and suggested it be part of a comprehensive grand strategy that incorporates various methods to address both the terrorist networks and potential supporters through all elements of national power.[35] Both direct and indirect deterrent efforts aimed at non-state actors provide legitimate methods to prevent terrorist attacks. However, those efforts that focus on the supply side fail to address the situation once proliferation has occurred. And, deterrence by denial strategies that hinge on defensive measures do not

---

[31]Dunn, *Deterrence and Nuclear Proliferation in the Twenty-First Century*, 36.

[32]Jeffrey W. Knopf, "Wrestling with Deterrence: Bush Administration Strategy After 9/11," *Contemporary Security Policy* 29, no. 2 (2008), 229–265., 251.

[33]Colby, "Expanded Deterrence: Broadening the Threat of Retaliation," 43–59, 58.

[34]Auerswald, "Deterring Nonstate WMD Attacks," 543–568, 547.

[35]Knopf, "Wrestling with Deterrence: Bush Administration Strategy After 9/11," 229–265, 258; Bowen, "Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism," 54–70, 69; Davis and Jenkins, "Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda," 86, xviii.

account for limited resources or the natural reactions of populations after an attempted attack. An effective deterrence by punishment strategy would fill these gaps; and, while the literature provides support for this method, it does not provide a framework for determining the appropriate punishment. The literature confirms that deterrence by punishment can play an important role in preventing attacks, if the policy clearly articulates a defined retaliation that threatens terrorists' centers of gravity in response for a specific type of attack. A valuable framework would address the difficult facet of proposing a comprehensible retaliation policy that incorporates all elements of national power. It would develop an attack reprisal doctrine that would effectively deter terrorists, yet be publically acceptable, while possessing some level of automaticity.

E. THEORETICAL FRAMEWORK

As the literature suggests, punitive deterrence is based on fear of retaliation, and that fear is generated by the risk of real loss. The key to deterring violent non-state actors is first to identify those elements the terrorist system can ill afford to lose then credibly signal the intent to retaliate against those elements should a terrorist group attack America. As a result, terrorists will weigh the benefits of attacking the United States against the losses they will sustain from that response. Consequently, U.S. deterrence strategy must send a message that clearly states the punishment that is directly associated with the undesired actions of non-state actors.

However, the level of response should be proportionally related to the type and destructive effects of an attack to be in tune with the level of public outrage the attack generates. Would the United States really impose the same punishment on a non-state actor committing cyber terrorism as it would for nuclear terrorism? A uniform policy towards all terrorism may signal the intent, but lack credibility. Jeffrey Knopf touched on this dilemma in his article "Wrestling with Deterrence" and suggested developing a "situation-specific" deterrence policy that would clearly articulate consequences for crossing specified red lines.[36] Furthermore, if current policy makes costs uniformly high,

[36]Knopf, "Wrestling with Deterrence: Bush Administration Strategy After 9/11," 229–265, 255.

it could unintentionally drive the terrorists toward larger more destructive attacks. In other words, since the intended response to terrorism does not vary by the type or magnitude of terrorist attack, terrorists' expected utility is directly proportional to the level of attack.

On the contrary, instead of correlating threats to undesirable actions, U.S. policy threatens all terrorism behavior with the same degree of punishment, which is unrealistic ex post. As David Auerswald notes, it is not clear that the current policy broadcasts a deterrent threat because it "vows to kill or capture terrorists regardless of whether they have attacked the U.S."[37] This methodology also runs contrary to standards of crime and punishment, where the level of punishment correlates to the degree of crime. Assuming the level of retaliation is proportionally constrained by the magnitude of attack and size of the terrorist organization, a limited terrorist attack orchestrated by a small and isolated group might require little to no military reprisal. In contrast, a nuclear detonation in Chicago by a large, complex network with state sponsorship more likely warrants a full military campaign. Nonetheless, U.S. policy signals the same punishment for terrorism that involves a car bomb attack in a foreign country as one that kills thousands in a U.S city.

F. METHODOLGY

U.S. policy documents provide information about the most current counterterrorism strategies that serve as potential threats of deterrence. These strategies would need to meet two criteria for them to signal credible deterrent threats. First, the methods must be *relevant* in the sense that they threaten effective targets for retribution—they must hold something the non-state actor covets at risk. Second, the threats must be *credible* in that the method of retaliation would be supported as a reasonable response to the undesired action. For the purpose of this study, U.S. policies reviewed were the most current at the time of writing. While they are subject to change with the new Obama

[37]Auerswald, "Deterring Nonstate WMD Attacks," 543–568, 546.

administration, it is anticipated that some elements of strategy will remain the same. In addition, the lessons learned from an analysis of Bush-era strategy can help inform future strategy.

To evaluate U.S. strategy under the first criterion, each of the counterterrorism methods is compared to a theoretical model of critical vulnerabilities of non-state actors. If these methods prove relevant to the identified vulnerabilities under this analysis, then current strategy contains effective punishment threats that can be examined under different attack scenarios to evaluate the second criterion—credibility. To evaluate the second criterion, the expected U.S. response is evaluated for dissimilar attack scenarios to demonstrate the lack of credibility. Specifically, the thesis compares retaliatory threats for cyber-terrorism and a nuclear attack. Showing that the signaled response holds constant for varying degrees of terrorism will highlight the potential un-believability of deterrent signals in current policy. This evidence in turn supports an argument for establishing a retaliation framework based on type of attack, as opposed to the simple fact of terrorist activity. In conclusion, the evaluated responses to both types of attack—cyber and nuclear—are used to demonstrate how a theoretical retaliation framework for deterring non-state actors would look.

G. THESIS OVERVIEW

Already covered in this introductory chapter is the background and purpose of the research, discussion and literature review on the topic of deterrence, and the theoretical framework and methodology of the analysis. Chapter II begins with analysis on the question of whether a state can deter non-state actors from committing undesirable actions. The ability to deter terrorists is a fundamental component of this thesis and vital to defining the "nodes-of-influence" that a deterrence strategy must threaten in order to manipulate decisions. From this discussion on influencing terrorists, critical components of retribution are identified in order to develop a set of terrorist vulnerabilities that align with their nodes-of-influence. Moreover, these nodes-of-influence comprise the Centers of Gravity (COGs) that U.S. counterterrorism strategies must target in order to constitute relevant threats of

retaliation. By evaluating the targets of recent policy on counterterrorism, this approach makes it possible to assess the relevance of current policy threats as possible responses to terrorist attacks in the following chapters.

Chapter III analyzes the potential targets and credible responses to a hypothetical terrorist attack on U.S. critical infrastructure. It begins with a review of relevant policy to establish a common frame of reference. The next section provides a narrative overview of the scenario to include general details of the event, participants, and consequences of the attack. Next, the scenario is analyzed to determine a list of potential targets to punish in retaliation for the attack. These targets are then compared to the objectives of U.S. counterterrorism strategy identified in Chapter II to determine if it effectively targets a node-of-influence. Finally, those policy threats corresponding to relevant targets are individually evaluated to determine their credibility as a method of retaliation for this scenario. The results are tabulated for comparison to those of the next chapter.

Chapter IV mirrors the previous chapter in format and intent, but is written in the context of a nuclear terrorist attack scenario. This chapter also consists of: a brief review of relevant policy, scenario overview, analysis of potential targets of retaliation, comparison of policy threats to scenario targets, and summary of results. The results are again tabulated for comparison to the results of the previous chapter.

The final chapter contains a compilation of the results and a comparative review of the credible retaliation options for each scenario. The comparison illustrates the differences in the expected response to differing types of terrorist attack, in order to support the argument that current policy does not signal credible threats of retaliation. This is an issue that must be resolved before the Unites States can put forth an effective deterrence strategy. This chapter closes with a policy recommendation to fill this gap by proposing a retaliation framework that signals credible deterrence threats by tailoring the response to the type of attack.

II. VALIDATION OF CURRENT POLICY THREATS

A. INTRODUCTION

This chapter assesses whether current counterterrorism strategies of the United States hold at risk the most relevant targets for retribution—whether credibly signaled or not. For this to hold true, its strategy must target those centers of gravity that will most influence a non-state actor's decisions. To carry out this assessment, this chapter begins with discussion of whether a threat of punishment has any impact on the decisions of violent non-state actors. If the potential to influence non-state actors' decisions does exist, then the next step is determining which factors hold the most weight in those decisions. Identifying what those actors hold dear produces a list of vulnerabilities that when credibly threatened will influence outcomes. Finally, if current counterterrorism strategies correlate with the vulnerabilities identified through this theoretical approach, then its methods constitute relevant threats.

The first part of this chapter explores the question of whether violent non-state actors react to influence exerted in the form of a deterrent threat. It discusses various theories on decision making to analyze how well they reflect the behavior of terrorist organizations. Determining which of the various behavior theories most accurately describes a non-state actor will help make clear whether or not such actors might be affected by deterrent threats. The next section identifies terrorists' "nodes-of-influence." Nodes-of-influence represent those components of the terrorist system that contribute to its decisions and affect its operations. In turn, these nodes represent these centers of gravity that need to be targeted in an effective retaliation framework. Therefore, potential vulnerabilities of the centers of gravity are derived from literature on counterterrorism strategy and deterring non-state actors. For the purpose of this study, current policy strategies will be deemed to contain relevant threats of retaliation if their targets align with these vulnerabilities.

To identify current deterrent threats, primary counterterrorism strategies are extracted from U.S. policy documents and followed with discussion on how well they

correlate to vulnerabilities of the nodes-of-influence. The last step compares these counterterrorism methods against the theoretical model developed later in this chapter—results tabulated in Table 1. In summary, this chapter intends to support claims that violent non-state actors have coveted desires and assets that when appropriately threatened cause them to make responsive decisions to avoid loss and, more importantly, to show that the current policies of the U.S. contain the relevant methods to target those vulnerabilities. To the extent these options are validated, their credibility can then be evaluated under hypothetical attack scenarios in subsequent chapters.

B. DETERRING VIOLENT NON-STATE ACTORS

As discussed earlier, to influence a non-state actor there must be a credible threat that holds something it values at risk. This risk emerges as a result of directing a threat towards a specific vulnerability (Threat + Vulnerability = Risk). Since threat is generated through the deterrent message, the undetermined variable is vulnerability. Theory on organizational behavior provides the most fruitful approach to identify non-state actors' nodes-of-influence which in turn yield vulnerabilities to threaten with retaliation.

To ensure clarity of the relationships and lexicon within this thesis, a diagram of the concept and related terms is shown in Figure 1. Boxes in dark grey represent how the vulnerabilities associated with components of an organization have a potential to influence non-state actors' decisions. The other boxes illustrate the steps involved in establishing a relevant threat—i.e., threatening targets associated with centers of gravity should cause a deterrent effect on the organization.

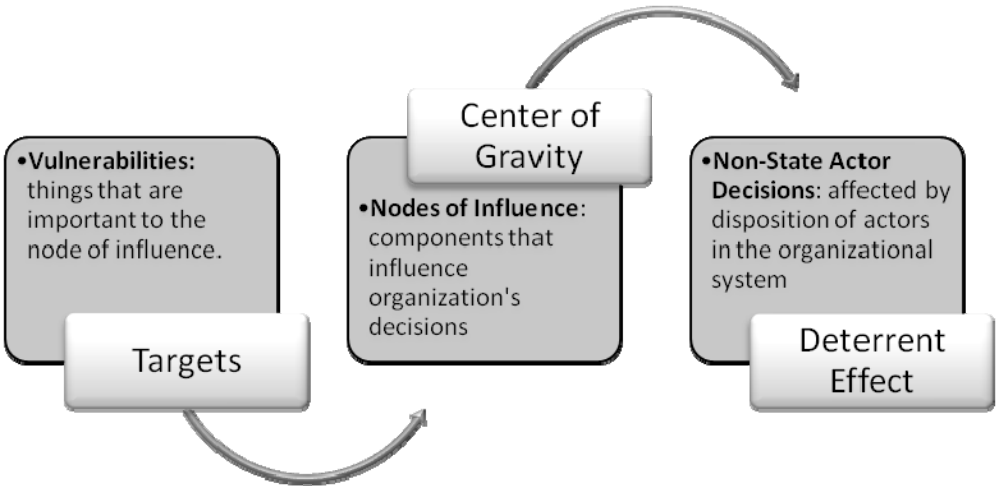

Figure 1. Threat transmission diagram

This concept must now be translated into an operational approach in order to identify actual components and vulnerabilities for non-state actors. Working this process in reverse, the first step requires analysis on influencing non-state actors' decisions. Based on that analysis, a representative model can be selected to provide "nodes-of-influence" for a non-state actor system from which to identify the associated vulnerabilities.

C. ANALYSIS OF NON-STATE ACTOR BEHAVIOR

This section discusses the rationality of terrorists, their group dynamics, and their organizational structure. The literature debates whether a violent non-state actor's behavior can be characterized as rational, thus raising questions concerning the possibility of deterring terrorists through threat of punishment. Rational, in this context, would describe a subject that operates with stable and transitive preferences, and that makes decisions based on expected utility. Opponents of this argument view terrorists as irrational, unpredictable actors that make decisions without regard to outcomes, and therefore impervious to deterrent threats. However, to assume that terrorists are irrational because they chose to attack powerful nation states or commit suicide attacks contradicts

evidence concerning terrorist organizations presented below. This presumption seems to focus more on fanatical terrorist operatives who execute the decisions and less on those involved in making them.

Regardless, a significant weakness of the classic rational actor approach, as Fearon points out, is that it does not consider the decision-makers' point of view when attempting to predict actions.[38] This might explain the tendency to discount terrorists as irrational objects because their actions do not fit neatly into a particular perception of rational choice. Similarly, Lebow is critical of rational choice deterrence theory because it fails to take into account how the initiator perceives and deals with risk. He claims that rational choice outcomes vary between actors who prefer to maximize gains and those that maximize loss, thereby changing how each calculates expected utility.[39] He goes on to state that, "whether or not an actor is rational is beside the point. Deterrence theory does not predict that initiators will be rational. It specifies the conditions under which rational initiators will choose not to attack."[40]

Putting this into the context of non-state actors, Alexander George points out that assumptions of rationality have historically proved limited in dealing with state leaders during previous conflicts and the Cold War—and there are additional limitations when dealing with non-state actors.[41] He presents seven specific characteristics (paraphrased below) evident in analysis of non-state actors that provide useful insight into this challenge of identifying adequate vulnerabilities to exploit.[42]

1. Unlike state leaders, non-state actors are not protecting geographical bound areas and infrastructure.
2. Behavioral patterns of non-state actors increase the difficulty in influencing their cost-benefit analysis.

---

[38]James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (Summer, 1995), 379–414, 395.

[39]Richard Ned Lebow and Janice Gross Stein, "Rational Deterrence Theory: I Think, therefore I Deter," *World Politics* 41, no. 2 (Jan., 1989), 208–224, 208–209.

[40]Ibid., 212.

[41]George, *The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries*, 325, 297.

[42]Ibid., 297–298.

3. Non-state actors lack organizational structure and clear lines of authority.
4. It is difficult to influence a group with coercive efforts because sub-actors may have opposing viewpoints.
5. Non-state actors have higher levels of motivation than the more dominant state.
6. Attempting to pressure other states to take action against the non-state actors is difficult.
7. Non-state actors exploit the coercing state's political and societal constraints.

Consequently, George posits that an actor-specific behavioral model provides a better approach for analysis of non-state actors.

From this perspective, the unitary-rational actor theory fails to universally define the decision making process of non-state actors. However, it may prove useful in predicting outcomes if the analysis takes the subject's prejudices into consideration rather than those of the analyst. The claim that non-state actors behave irrationally only addresses the non-traditional value its leader assigns to costs and benefits. None of the counterarguments refute that, through some process, they weigh options to determine relative advantage. Rationality is relative to one's point of view in that actions of a terrorist may appear irrational to the observer yet quite logical to the subject. Evidence that terrorists consider expected utility is found in a statement by Hamas leader M. Al Sahar: "We must examine the costs and benefits of continued armed operations."[43] Therefore, applying theory of rational choice to non-state actors could prove beneficial in predicting behavior of specific individuals of an organization, but used alone would limit the target opportunities to those efforts aimed at goals of individuals and not the collective.

Janis provides another possible model for non-state actors that describes how "groupthink" characteristics of a decision making body affect outcomes. Hart explains three characteristics associated with groupthink as "those producing an overestimation of the group (illusion of invulnerability; belief in inherent morality), those producing closed-mindedness (collective rationalizations; stereotyped images of out-groups), and those

[43]E. Berman, "Hamas, Taliban and the Jewish Underground: An Economist's View of Radical Religious Militias," *SSRN Working Paper Series* (Oct, 2003), 1.

producing pressures toward uniformity (self-censorship; illusion of unanimity; direct pressures on dissenters; self-appointed mindguards)."[44] This work could provide valuable insight into the dynamics of terrorist groups with respect to interactions between a radical leader and close advisors or the camaraderie of a terrorist cell. However, it fails to represent other important components of the decision process, especially those entities enabling a non-state actor to operate. If terrorism is the product of a network or a system, parts of the network that are not part of the inner circle will be less susceptible to groupthink and therefore more likely to be influenced by costs and benefits.

Lastly, Allison's bureaucratic politics model describes a process wherein the decision of an organization comes not from a single rational actor, but more as a result of bargaining among its members. Important to note, he states that its members (bureaucrats) are rational actors motivated by what is best for themselves and their organization.[45] These "bureaucrats" use their specialized knowledge and asymmetrical information to manipulate decisions. Allison posits that an organization's decisions are influenced on the front-end, then manipulated during execution as a result of members' ability to assert influence on the outcomes. This would suggest that applying deterrent measures to control or alter this information-flow and influence would affect the organization's decision process. Consequently, Allison claims that it is important to identify "action channels" when attempting to predict decisions.[46] Such channels would constitute those common players and established procedures involved in the decision process.

Applying this concept to non-state actors would imply that, within a terrorist organization, multiple players at various layers influence the group's decisions based on their perceptions and desired outcomes. Analyzing some of the statements and policies

---

[44]Paul't Hart, "Irving L. Janis' Victims of Groupthink," *Political Psychology* 12, no. 2 (Jun., 1991), 247–278, 259.

[45]Graham T. Allison and Morton H. Halperin, "Bureaucratic Politics: A Paradigm and some Policy Implications," *World Politics* 24, no., Supplement: Theory and Policy in International Relations (Spring, 1972), 40–79, 43.

[46]Ibid., 45.

of Al Qaeda provides evidence that non-state actors behave in similar fashion. As described by a Congressional Research Service Report, within Al Qaeda there are elements that have taken on the form of an organization with internal bureaucracy:

> Following the death of Abu Musab al Zarqawi in 2006, leading Al Qaeda affiliates established an entity known as the Islamic State of Iraq based in Iraq's western Al Anbar province. The group's leaders, Abu Umar al Baghdadi and Abu Hamzah Al Muhajir, have since released a number of statements outlining the policies and goals of the new 'Islamic state' and attacking a number of Iraqi groups. A ten-member cabinet was announced in April 2007.[47]

That same report described an example of "bureaucratic competition" after Osama Bin Laden had condemned Arabs supporting Iraqi and coalition forces to suffer the same violent persecution as non-Arabs. Subsequently, his top lieutenant, Al Zawahiri, and al Qaeda in Iraq leader Al Zarqawi demonstrated differing opinions on the outcome of targeting fellow Muslims based on secular affiliation. "These differences became public in October 2005 after the publication of an intercepted letter reportedly written by Al Zawahiri to Al Zarqawi in which Al Zawahiri offered advice to Al Zarqawi on his campaign in Iraq. Specifically, Al Zawahiri questioned the wisdom of pursuing a campaign against Shiite Iraqis on a sectarian basis when sectarian violence may reduce overall public support among the region's Sunni Muslim population for Al Qaeda's objectives."[48] Such strategy debate between Al Qaeda's "bureaucrats" despite direction from the organization's leader (Bin Laden) suggests that organizational behavior theory would provide useful analysis for non-state actors.

Why is this important? If it were true that a leader independently makes decisions that are explicitly executed by the entire terrorist organization, then all efforts to influence outcomes should focus exclusively on the leader. On the contrary, assuming that bureaucratic theory applies to a non-state actor's decision process, then each bureaucratic node would translate into points against which to apply pressure with the

[47]Christopher M. Blanchard, *Al Qaeda: Statements and Evolving Ideology* (Ft. Belvoir: Defense Technical Information Center,[2006]), www.dtic.mil (accessed 8/10/2009), 9.

[48]Ibid., 8–9.

purpose of influencing the overall outcome. In other words, sub-actors within a terrorist network (based on their own desires, interpretations, and economic analysis) influence the organizational decisions that provide numerous avenues to assert influence. This concept should incorporate those external entities supporting the group's ability to sustain operations as well. For example, elements providing safe havens, training, financial and material support to al Qaeda will attempt to influence the organization's decision process as each would have personal interests and desires vested in the outcome. To conclude, it is not necessary to assume perfect rationality. If terrorists strategize or even consider outcomes when making decisions, and are at all sensitive to costs, they can be influenced.

D. THE NON-STATE ACTOR SYSTEM

Through the lens of organizational theory, violent non-state actors resemble a network of bureaucrats that can be influenced by threatening the group's organizational goals and the individual interests of its members. For these reasons, organizational theory provides the best model for determining methods to influence a non-state actor's cost-benefit analysis because it provides a framework that encompasses the full spectrum of vulnerabilities. Therefore, a strategy that employs methods to raise operational costs associated with these vulnerabilities would provide relevant targets for a deterrence policy.

Considering non-state actors as organizations, Davis and Jenkins provide a representative model of the structure of a terrorist network, which they use as the basis for recommending an influence strategy. Their strategy "emphasizes the fact that terrorists in a given group operate within a much larger system, some elements of which are potentially more vulnerable than others."[49] The work provides a fundamental and well-documented breakdown of the critical actors in a terrorist system (Figure 2) based on an organizational system approach.

[49] Davis and Jenkins, "Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda," 86, 14.

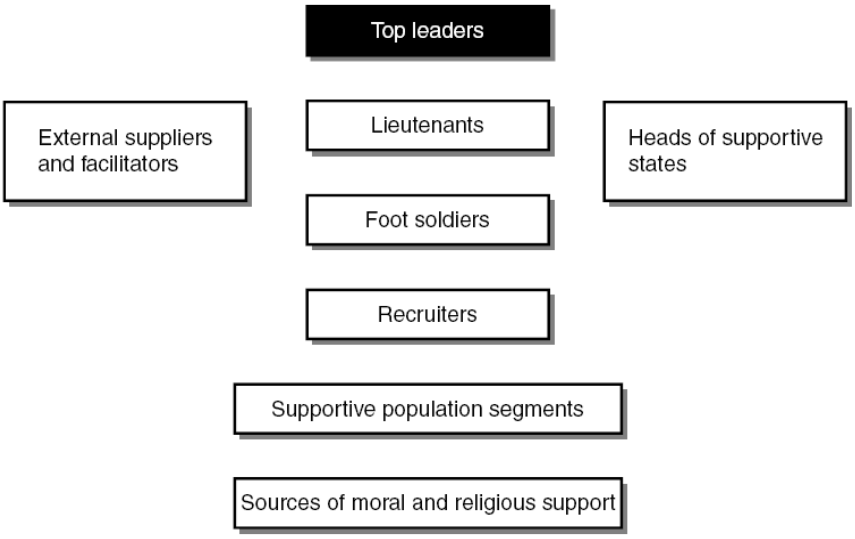

Figure 2. The actors in a terrorist system (From Davis and Jenkins)[50]

Moreover, the targets identified in this model represent a non-state actor's decision-makers and bureaucracy of the organization. These actors provide the nodes-of-influence whose vulnerabilities should be threatened to establish an effective deterrence policy.

E. VULNERABILITIES OF THE NON-STATE ACTOR SYSTEM

Retaliation is the most important aspect of punitive deterrence, encompassing a wide range of alternatives to threaten those one seeks to deter. And, threatening vital nodes of the terrorist organization is the critical component of retaliation. On one end of the spectrum, retaliation can take the form of law enforcement and judicial action to prosecute those caught through normal law enforcement processes. On the other, the military could be employed to force regime change, as in the case of Operation Enduring Freedom in Afghanistan. This section explores methods to attack vulnerabilities associated with the nodes-of-influence identified above.

[50]Davis and Jenkins, "Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda," 86, 15.

Intense examination of how a group operates, trains, communicates, and maintains funding provides information necessary to identify and threaten all critical nodes—not just the bombers. Eric Herren argues that "we have to confront suicide terrorism at its origin, with the mastermind behind the attack—the trainers, the bomb factory and the terrorist shelters."[51] Hypothetically, analyzing a situation wherein Israel continues to sustain rocket attacks and suicide bombings, such a situation would imply that past forms of Israeli retaliation had not sufficiently deterred the enemy. One possible explanation might be that the targets of retaliation are not sufficient centers of gravity because groups launching attacks do not rely exclusively on internal support. This might imply that some third party or even one or more nation states could be supporting the terrorists. Taking into consideration the retaliatory concept described above, deterring terrorist attacks on Israel would require a more holistic approach that threatens all of the elements required to sustain the violent campaign.

Several approaches have been developed on this subject, and range from single focus strategies like attacking ideology to multi-faceted comprehensive strategies. As some studies suggest, leaders are vulnerable to attacks on organizational goals like those published by Al Qaeda or the Brotherhood of Islam. For example, Gary Servold notes that the Brotherhood of Islam had six main objectives and three long-term goals that could be threatened.[52] Trager and Zagorcheva claim that even highly-motivated terrorists can be influenced by threatening their local agenda rather than individuals' preservation.[53] However, solely focusing on the leader may limit retaliatory options to a single rational-actor approach opposed to an organizational approach. Therefore, additional methods would be necessary to attack vulnerabilities of the remaining actors and support networks.

---

[51] Eric Herren, "Counter-Terrorism Dilemmas," International Institute for Counter-Terrorism, http://www.ict.org.il/articles/ (accessed 6/1/2009).

[52] Gary M. Servold, "The Muslim Brotherhood and Islamic Radicalism" In *Know Thy Enemy: Profiles of Adversary Leaders and their Strategic Cultures*, eds. Barry R. Schneider and Jerrold M. Post, 2nd ed. (Maxwell Air Force Base, AL.; Wash. D.C.: USAF Counterproliferation Center, 2003), 41, 56.

[53] Trager and Zagorcheva, "Deterring Terrorism: It can be done," 87–123, 88.

A more effective strategy should derive targets from various vulnerabilities associated with the entire organizational structure. These diverse strategies propose attacking objectives related to factors that enable a terrorist organization to thrive. In a RAND study on counterterrorism, Blanchard suggests a four-prong strategy that globally attacks jihadist ideology, severs group links, denies sanctuaries, and provides support to states confronting local jihadist threats.[54] Similarly, when testifying before Congress, Bruce Hoffman identified five elements of a counterterrorism strategy that include neutralizing the enemy, countering propaganda, and denying support.[55] Colby proposes expanding the threat of retaliation to all those responsible: "supporters, facilitators, moneyman, back office workers, infrastructure, housing, food and other supplies, land, political control over territories, marks of prestige and so forth."[56] Whiteneck also suggests that deterrence should target societal elements and third-party supporters—like networks of financiers, supporters, scientists, and smugglers.[57] He claims that "making the general populations aware that they might pay a large proportion of the costs of a terrorist attack against the United States may support the larger deterrent aims."[58] The counter to this argument contends that punishing non-complicit civilians only serves to legitimize the terrorists and strengthen their local support.[59] To summarize, the literature suggests using methods to target vulnerabilities of the entire system through various means of punishment to maximize the deterrent effect.

F. EVALUATION OF RECENT U.S. POLICY

The counterterrorism strategies found in the 2006 National Strategy for Combating Terrorism provide methods that the United States is employing against known

---

[54] Angel Rabasa and others, *Beyond Al-Qaeda. Part 1. the Global Jihadist Movement* (Santa Monica, CA: RAND Corporation,[2006]), www.dtic.mil (accessed 7/14/2009), 160.

[55] House International Relations Committee, *Does our Counter-Terrorism Strategy Match the Threat?* CT-250 sess., 2005, 1–20, www.dtic.mil (accessed 7/14/2009), 15.

[56] Colby, "Expanded Deterrence: Broadening the Threat of Retaliation," 43–59, 49.

[57] Whiteneck, "Deterring Terrorists: Thoughts on a Framework," 187–199, 194.

[58] Ibid., 197.

[59] Bowen, "Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism," 54–70, 63; Auerswald, "Deterring Nonstate WMD Attacks," 543–568, 551.

terrorists. Found within the document's list of long- and short-term objectives are several areas that potentially align with nodes for influencing non-state actors discussed above. These include targeting terrorists, financial components, means-of-communication, state support, and safe havens, waging a battle of ideas, and countering propaganda.[60] The long-term strategy seeks to win the "war of ideas" through the spread of democracy to promote basic rights and freedoms for all people. The goal is to counter the political alienation, injustices, subculture of misinformation, and radical ideology that cause the spread of terrorism.[61] On the other hand, the short-term strategy focuses on preventing terrorist attacks by targeting the personnel and infrastructure of terrorist networks. It emphasizes targeting the leaders to weaken the organization, prosecution of foot soldiers, disrupting recruitment, targeting communication and propaganda operations, and disrupting the flow of funds and weapons to terrorists.[62] It also addresses terrorist's means-of-travel and entry into the U.S. as a way of disrupting operations. However, for any corporate entity requiring access to the U.S. for business, this could also serve as a threat of punishment for third-party support. Furthermore, the Strategy to Combat Weapons of Mass Destruction alludes to the possibility of nuclear response in retaliation against guilty states and clearly signals intent to violate sovereignty with full military engagement. These two documents provide the preponderance of policy guidance on counterterrorism efforts and signal the intentions of the United States. Each of these methods is discussed in greater detail below to assess its relationship to vulnerabilities of the nodes-of-influence.

1. Finance

The first targeted vulnerability deals with financial support to non-state actors. Terrorist networks require a significant amount of funding to sustain infrastructure,

---

[60] Executive Office of the President, *National Strategy for Combating Terrorism* (Washington, D.C.: The White House, [2006]), 9–17.

[61] Raphael F. Perl, *National Strategy for Combating Terrorism: Background and Issues for Congress* (Ft. Belvoir: Defense Technical Information Center,[2007]), http://handle.dtic.mil/100.2/ADA473792. (accessed 8/26/2009), 5.

[62] Ibid., 3.

operations, training, and logistics. Hence, attacking formal financial channels would force terrorists to rely on informal methods which slow and degrade their processes.[63] Areas may include targeting of charities, financial institutions, and material suppliers with actions to freeze assets, block transfers, and deny access to U.S. markets.[64] As Levitt points out, attacking financial systems can deter "non-designated parties" from financing terrorists for fear of losing business, personal wealth and their reputations.[65]

Non-state actors also utilize western nations for fund raising, material purchases and furthering political agendas. For example, American charity organizations like the Holy Land Foundation and Muslim Arab Youth Association provided support to Hamas and families of suicide bombers, deportees and detainees.[66] There is no question that laws of the state impact non-state actors' fund raising activities, especially in the more permissive European countries.[67] Davis recommends cutting off and exposing charities that support terrorist organizations and prosecuting those that knowingly finance terrorism.[68]

Another important mechanism to combat terrorist finances is establishing a mechanism to globally block financial channels and seize funds of these organizations. For example, the United States successfully froze large amounts of Al Qaeda finances initially, but later lost control and funds started slipping back into the network. According to a *Washington Post* article, "in the months immediately following the 9/11 attacks, the United States and other U.N. members moved to shut down Al Qaeda's

---

[63] Matthew Levitt and Michael Jacobson, "The U.S. Campaign to Squeeze Terrorists' Financing," *Journal of International Affairs.* 62, no. 1 (Fall, 2008), 67–85, 80.

[64] Davis and Jenkins, "Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda, 86," 21.

[65] Levitt and Jacobson, "The U.S. Campaign to Squeeze Terrorists' Financing," 67–85, 81.

[66] R. Schneider and Jerrold M. Post, eds., *Know Thy Enemy: Profiles of Adversary Leaders and their Strategic Cultures*, 2nd ed. (Maxwell Air Force Base, Ala.: USAF Counterproliferation Center, Air War College, Air University, 2003), 325, 62.

[67] Daveed Gartenstein Ross, Joshua D. Goodman and Laura Grossman, *Terrorism in the West 2008 a Guide to Terrorism Events and Landmark Cases* (Washington, DC: FDD's Center for Terrorism Research,[2009]), http://www.hsdl.org/hslog/?q=node/4972 (accessed 8/10/2009), 3.

[68] Davis and Jenkins, "Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda," 86, 28–29.

financial network, freezing more than $112 million in assets."[69] However, the report goes on to say that despite these initial successes for counterterrorism efforts, al Qaeda has been able to maintain revenues streams of at least $30 million (with some estimates as high as $300M) from sources in Africa and Asia.[70]

2. Communications and Propaganda

According to principles of war, one of the most critical targets is the enemy's command and control systems. One method to target command and control is disrupting critical communication-links between terrorist leaders, commanders, financiers, and operatives. This requires identifying and either isolating or taking control of terrorists' means of communication, such as their access to the Internet, cell phones, and land lines. Admittedly, this is more difficult to accomplish against clandestine opponents that are integrated into mainstream societies or isolated in some remote area of the globe. However, it is clear that Al Qaeda has used faxes, audio-visual recordings, and the Internet for propaganda and communication for the past decade.[71] Attacking available modes of communication would have a devastating effect on the group's ability to conduct further operations. For example, "global counterterrorism operations in the aftermath of the September 11, 2001, terrorist attacks appear to have limited Bin Laden's ability to provide command and control leadership to Al Qaeda operatives and affiliated groups."[72]

Increasingly, the Internet has become the primary conduit for terrorist communications because it allows them to operate without personal exposure.[73] "When

---

[69] Colum Lynch, "War on Al Qaeda Funds Stalled. Network 'Fit and Well,' Ready to Strike, Draft of UN Report Says," *Washington Post*, sec. A, August 29, 2002, 2002, http://www.highbeam.com/doc/1P2-382734.html (accessed 8/10/2009).

[70] Colum Lynch, "War on Al Qaeda Funds Stalled. Network 'Fit and Well,' Ready to Strike, Draft of UN Report Says," *Washington Post*, sec. A, August 29, 2002, 2002, http://www.highbeam.com/doc/1P2-382734.html (accessed 8/10/2009).

[71] Blanchard, "Al Qaeda: Statements and Evolving Ideology," 1–18, 1.

[72] Ibid., 2.

[73] Homeland Security Council, *National Strategy for Homeland Security* (Washington, D.C.: Executive Office of the President, [2007]), 4.

one looks at the recent attacks in Madrid and London, for example, it becomes clear that whether or not these cells were formally 'connected' to high-level jihadist operatives, these types of operations are analyzed and debated on jihadist Web sites and online forums."[74] Internet sites boasting jihadist and Salafist propaganda promoting radicalism and advocating violence should be targeted with cyber-warfare methods. Brimley claims that countering the propaganda message should not forgo efforts to prevent its dissemination by blocking communication channels.[75] Moreover, attacking terrorist means of promoting their agenda and violence would stifle them from achieving their political goals, another targeted vulnerability to be discussed later.

3. Terrorist Network

The process of attacking the network involves various methods to target individuals within the terrorist organization. The purpose is to remove leaders and operatives from the network through law enforcement and military action. This will degrade the network, demoralize the members, and diminish the organization's ability to conduct operations and recruiting.[76] Although some argue the ineffectualness of killing or capturing terrorist leaders because they are easily replaced by lieutenants, the validity of this argument is unclear. Regardless of how fast someone steps into that leadership position, it is highly probable that the organization will suffer some sort of setback. Also, a policy that threatens to kill or capture terrorist leaders will influence their decisions out of concerns for self-preservation. It is evident that U.S. efforts to get Bin Laden have had a tremendous effect on his patterns, which degrades his ability to control the Al Qaeda organization. After an evaluation of Bin Laden's truce offer in 2006, most experts claimed that he lacked the power to convince the sub-networks of Al Qaeda to withdraw

[74] Shawn Brimley, "Tentacles of Jihad: Targeting Transnational Support Networks," *Parameters: Journal of the US Army War College* 36, no. 2 (2006), 30–46, www.dtic.mil (accessed 7/18/2009), 36.

[75] Shawn Brimley, "Tentacles of Jihad: Targeting Transnational Support Networks," *Parameters: Journal of the US Army War College* 36, no. 2 (2006), 30–46, www.dtic.mil (accessed 7/18/2009), 35–36.

[76] Davis and Jenkins, "Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda," 86, 24.

from hostilities.[77] The possibility that non-state actor systems are loosely organized highlights the importance of targeting the entire system and not just its leaders.

Targeting operatives and complicit members also provides a deterrent effect by influencing the organization's operational elements. Again, potential methods would involve killing or capturing complicit members, but capturing may produce the most effective results for radical members with martyrdom desires.[78] Arresting operational level terrorists and convicting them in a judicial system deprives them of benefiting from martyrdom and criminalizes their political aims. Such second order effects could multiply if conviction is achieved within the judicial system accepted by the non-state actor rather than Western courts.

4. Countering Political Goals

Analyzing the strategic goals of a non-state actor may make it possible to target their political agenda. Promoting democracy, attacking ideology with counter narratives, providing support to opposing regimes, and supporting moderate religious leaders are potential methods to attack political goals of terrorists. Again turning to statements by Al Qaeda leaders, it is clear that Al Zawahiri fervently opposes the establishment of democracies in Iraq and Afghanistan, and Al Zarqawi denounced Sunni participation in Iraq's new government while condemning Shiite political organizations.[79]

Terrorists wage war in the psychological realm and place enormous effort towards reaching the public with their message. "Bin Laden and his deputies have personally stated their belief in the importance of harnessing the power of international and regional media for Al Qaeda's benefit, and Al Qaeda's central leadership structure has featured a dedicated media and communications committee tasked with issuing reports and

[77] Blanchard, "Al Qaeda: Statements and Evolving Ideology," 1–18, 2.

[78] Report by the National War College Student Task Force on Combating Terrorism, *Combating Terrorism in a Globalized World* (Washington, D.C.: National War College,[2002]), www.au.af.mil/au/awc/awcgate/ndu/n02combating_terrorism.pdf (accessed 10/18/2009), 44.

[79] Blanchard, "Al Qaeda: Statements and Evolving Ideology," 1–18, 8.

statements in support of the group's operations."[80] Attacking ideology with counter-narratives and disrupting communications would prevent the spread of ideology and work to discredit the message, both of which impair recruiting efforts. Therefore, non-state actors would have to consider the negative impact on their political agendas before committing to terrorism. Even for those groups already in conflict with American interests, it would have to be clear that the level of opposition to their political goals would significantly increase after an attack on the United States.

Another way to target political aims is to provide incentives and support to those regimes that counter the goals and activities of the non-state actor.[81] Evidence showing the importance of state actions to the goals of terrorists is found in statements by Bin Laden. "In 2004 and 2006, Bin Laden personally addressed the governments and citizens of Europe and the United States directly in an effort to discourage further support for their respective foreign policies in the Islamic world."[82] Furthermore, successfully supporting the opposing regimes can cause the terrorists to turn on the population for not revolting, as in the case of Bin Laden's criticism of the Islamic world for not answering the call to arms.[83] This technique also pertains to providing support to moderate religious leaders of the terrorist's sect, but who oppose violent expression.

5. Non-State Support

While efforts to destroy the terrorist organization, its means of communication, its finance, and its political goals cause significant damage to the operational system, they must be accompanied by efforts to also target supporting elements that turn organizational desires into reality.[84] Non-state support is one such element that enables

[80] Ibid., 1.

[81] Trager and Zagorcheva, "Deterring Terrorism: It can be done," 87–123, 109.

[82] Blanchard, "Al Qaeda: Statements and Evolving Ideology," 1–18, 6.

[83] Ibid., 5–6.

[84] Brimley, "Tentacles of Jihad: Targeting Transnational Support Networks," 30–46, 31.

terrorists to survive, thrive, and operate by providing resources, training, safe havens, and linkages to criminal networks. Three subgroups of targets emerge from this category: supporting communities, businesses, and criminal organizations.

It is often repeated that "all politics is local;" likewise, threats aligned with local issues could degrade community support. Popular support from within the umma (seamless community) provides funding, a recruiting base, and legitimacy to threaten others. Otherwise, terrorists must rely on states for support, which opens the door for state-level deterrence.[85] Bin Laden has promoted the importance of local support with his repetitive appeals to "the silent ulema" (religious scholars), businesses, and community leaders to establish an alliance.[86] Counter-societal targeting involves the use of kinetic and non-kinetic forms of retaliation against a populace for the purpose of deterrence. Methods to influence these communities include controlling foreign aid, seizure of local assets for reparation, sanctions, business restrictions, visa denial, and destroying critical infrastructure.

Furthermore, there exists a parallel, but covert, support network of criminal organizations that clandestinely provide weapons, materials, and funding sources to non-state actors. "Terrorists use gangs, drugs, prisons, money laundering, and smuggling networks to facilitate everything from recruitment to financing, material procurement, and operational support in the absence of a convenient state sanctuary."[87] Moreover, as difficult as it is to infiltrate a jihadist terrorist network, law enforcement agencies have been very successful when it comes to prosecuting operations against criminal organizations.[88] Therefore, targeting criminal elements that support terrorists provides an effective method of deterring third party support.

---

[85] Bryan S. Kohn, *Attacking Islamic Terrorism's Strategic Center of Gravity* (Ft. Belvoir: Defense Technical Information Center,[2002]), www.dtic.mil (accessed 7/14/2009), 6.

[86] Blanchard, "Al Qaeda: Statements and Evolving Ideology," 1–18, 7.

[87] Brimley, "Tentacles of Jihad: Targeting Transnational Support Networks," 30–46, 33–34.

[88] Ibid., 41.

6. State Support

Retaliating against states that support terrorism is more straightforward, and incorporates military and diplomatic efforts to impose economic sanctions, destroy infrastructure, and force regime change. Historic examples include economic sanctions on Iran for supporting Hamas, reparations from and air strikes on Libya, missile attacks on Sudan and Afghanistan for their support to Al Qaeda's attack on U.S. embassies, and overthrow of the Taliban for their connection with the attacks on 9/11. While the other targets being discussed can be difficult to identify or impose enforcement on, states are geographically bounded and possess easily identifiable targets to strike in retaliation. For this reason, deterring state support appears to yield the most effective and straightforward threat, which increases the importance of methods that cut off non-state support.

Additionally, since no organization in the world is purely self-sustaining, a second order effect may emerge where nations, financial institutions, and other entities begin to police terrorist activities for fear that they find themselves on the receiving end of retribution. The key is to isolate terrorist organizations, choke off their resources and drive them to extinction. For example, consider a hypothetical scenario in which a terrorist organization plans to use a particular country for safe haven, a certain financial institution to transfer funds, and a specific business as cover to travel to the U.S. for the purpose of detonating a nuclear bomb. Now, suppose the known policy of the U.S. is that a nuclear attack on our homeland invokes all means necessary to execute the following forms of retaliation: military retaliation against the supporting state, punishing all financial institutions involved, and destroying the culpable businesses. Then, intuitively self-preservation will discourage nations from providing weapons and safe havens to terrorists, financial institutions will rigorously monitor transactions, and foreign companies will better scrutinize employees that travel to the U.S. In other words, deterrence helps prevent terrorism by threatening to destroy those third-party elements necessary for terrorist organizations to operate.

7. Nuclear Retaliation

The last form of retaliation and by far the most controversial involves state and counter-societal targeting. Although this could be conducted to a lesser extent with conventional weapons, traditional deterrence methods threaten nuclear retaliation. In order to utilize nuclear weapons in retaliation for an attack, the punisher would have to not only be certain of attribution, but also with some level of conviction attribute blame to the supporting society as nuclear weapons do not discriminate. Experts like Stephen Younger mostly agree that nuclear weapons serve only to deter states and present an ineffective tool for deterring non-state actors.[89] Obviously, nuclear retaliation has very limited applications like response to a WMD attack, but still warrants deliberation when establishing deterrence policy. This issue is revisited in discussion of the nuclear attack scenario when analyzing probable U.S. response options.

Congruent across all of these strategies is that their efficacy depends upon gaining knowledge of the enemy. As Sun Tzu, the great Chinese strategist, once postulated, "By perceiving the enemy and perceiving ourselves, there will be no unforeseen risk in any battle."[90] Information gathered on actual non-state actors would provide the specific details on a terrorist organization that are needed to execute these retaliation methods on real targets. Nevertheless, a deterrence policy only has to make the reality of punishment self-evident to non-state actors.

G. COMPARISON OF POLICY THREATS TO VULNERABILITIES

To validate current policy strategy, the aforementioned threats are compared to targets of retaliation from the theoretical model above. Below, the vulnerabilities extracted from literature on deterring terrorism are correlated to their associated centers

[89] Stephen Michael Younger, *The Bomb: A New History*, 1st ed. (New York: Ecco Press, 2009), 238, 208.

[90] Sunzi and J. H. Huang, *Sun Tzu: The New Translation* [Sunzi bing fa.], 1st ed. (New York: Quill, 1993), 299, 52.

of gravity from Davis and Jenkins' model to establish targets of retaliation. Next, current counterterrorism methods from U.S. policy are compared to those targets to determine effectiveness. Table 1 illustrates the results of this qualitative comparison.

Terrorist Centers of Gravity **(Nodes-of-influence)**	**Targets of Reprisal** **(Vulnerabilities)**	**Recent U.S. Policy Threats** **(U.S. Counterterrorism Strategies)**
-Influence the organization's decision makers (Leaders/Lieutenants)	Attack political goals & ideology	-Democracy (promote rights and freedoms) -Battle of ideas (counter-narrative campaign) -Terrorist network (kill or capture members)
-Influence those that execute the operations (Foot soldiers)	Attack terrorist system	-Terrorist network (kill or capture members) -Communications (disrupt command and control)
-Counter efforts to elicit support and recruit membership (Recruiting)	Counter terrorists' propaganda	-Propaganda (counter-narrative campaign) -Communications (cyber warfare)
-Discourage financial support and disrupt financial transactions (Financiers)	Attack supply of funds	-Finance (seize assets, penalize donators, etc.) -Communications (charity advertisements) -Travel (restrict business travel to U.S.)
-De-legitimize religious base for radicalism and terrorism (Religious figures)	Counter radical ideology	-Battle of ideas (counter-narrative campaign) - Democracy (promote rights and freedoms)
-Isolate terrorists from state support and deny them sanctuaries (Rogue states)	Attack supporting nation states	-State support (economic sanctions/insurgency) -Safe havens (locate and destroy) -Military (regime change/nuclear retaliation)
-Isolate terrorists from community support and anonymity (Popular or non-state support)	Attack societal supporters	-Counter-societal targeting -Finance (seize assets, cut-off aid, etc.) -Travel (restrict access to U.S.)

Table 1. Comparison of theoretical targets and policy threats

As evidenced by the table, the current threats contained in U.S. policy effectively target most of the vulnerabilities that were identified as having the potential to influence a non-state system. For example, an effective counter narrative strategy aligns with targeting radical propaganda, which impacts the non-state actor's ability to recruit.

One problem with using these counterterrorism strategies for deterrence is that the United States currently employs these methods no matter what terrorists do. This is in contradiction to a principle of deterrence noted by Thomas Schelling, which points out that effective deterrence not only requires a threat of punishment for aggression, but also a promise of restraint for compliance.[91] For example, the United States has continued to persecute al Qaeda with all of the counterterrorism strategies discussed above regardless of their current activities, which gives them little incentive to consider future restraint. Conversely, the fact that, since al Qaeda's attack, the United States has been continually delivering punishment does help show resolve to any other non-state actors considering future attacks.

Clearly, after an attack, deterrence requires the United States to deliver promised retaliation to reestablish a deterrence posture. However, a broad strategy of seeking to eradicate all global terrorism does complicate efforts to institute a strategy aimed at deterring non-state actors yet to commit an attack. For the latter, a deterrence posture will require finding ways to signal limits on U.S. actions against groups that do not attack the U.S. homeland or cross other U.S. red lines, combined with a commitment to execute retaliatory responses if a new group does carry out an attack. In the case of al Qaeda, the United States could continue to pursue and persecute those leaders, operatives, and third party supporters involved in the 9/11 attacks, while promising to leave other financiers and community and government sympathizers alone providing there are no further attacks on the Unites States. Otherwise, future deterrence of al Qaeda would have to rely on escalatory threats where punishment invoked in response to 9/11 would be taken to a

[91] Thomas C. Schelling, *Arms and Influence*, (New Haven: Yale University Press, 1966), 74.

new level for a subsequent attack. With either of these strategies, U.S. deterrence policy must include some promise of restraint if non-state actors refrain from attacking U.S. interests, or the terrorists will see no benefit for compliance.

H. CONCLUSION

Arguably, the most difficult challenge in forming a credible retaliation policy for non-state actors is identifying exploitable vulnerabilities. The deterrer must identify actors that constitute the nodes which influence decisions and operations of the terrorist organization. As Figure 1 illustrated, effectively targeting the vulnerabilities of each node should have an effect on the organization's decisions. Non-state actors must maintain key elements of survival: safe havens, anonymity, financial backing, means of travel, and means of communications, to name a few.[92] These vulnerabilities provide targets to threaten with retaliation by all elements of national power: diplomacy, intelligence, clandestine operations, law enforcement, economic policy, foreign aid, public diplomacy, and homeland defense.[93] As a result of these threats, non-state actors will weigh the benefits of attacking the U.S. against the losses they will sustain from that response. The main target of this deterrence is non-state actors that have yet to attack the United States. Once the line has been crossed, deterrence has lapsed, and the violator becomes the target of retaliation.

To summarize, this chapter supports the claim that non-state actors have goals and assets that, when appropriately threatened, could cause them to make responsive decisions to avoid loss. Also, the results of this theoretical approach suggest that current U.S. policy does contain relevant targets for retaliation against appropriate vulnerabilities of terrorist centers of gravity. However, it is important to point out that there are limits to the availability of targets based on U.S. public support. As with any strategy, the nation's population must be willing and able to achieve its objectives. For example, striking a

---

92 Kean Commission, "9/11 Intelligence Failure" In *Intelligence and National Security: The Secret World of Spies: An Anthology*, eds. Loch K. Johnson and James J. Wirtz, 2nd ed. (New York: Oxford University Press, 2008), 417–458, 428–430.

93 Ibid., 418.

societal target may have a desirable impact on an important center of gravity, but public support could constrain that option based on how it judges the morality of such reprisal. Therefore, signaling a method of reprisal that does not meet this parameter undermines the credibility of threat and therefore fails to meet the prerequisites for deterrence. Therefore, the next step in evaluating the U.S. deterrence posture is to analyze the credibility of these deterrent threats from this perspective.

THIS PAGE INTENTIONALLY LEFT BLANK

III. EVALUATION OF RESPONSES FOR A CYBER ATTACK

> Safeguarding the American people also includes the preservation of the Nation's critical infrastructure and key resources (CI/KR). As set forth in the 2006 National Infrastructure Protection Plan (NIPP), critical infrastructure includes the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government. By protecting CI/KR, we further protect the American people and build a safer, more secure, and more resilient Nation.
>
> The 2006 National Strategy for Homeland Security[94]

A. INTRODUCTION

In August of 2003, an isolated problem at an Ohio utility company cascaded into power outages across eight states and most of Ontario, Canada, leaving 50 million people without power for several days. The "Northeast Blackout of 2003," as it was termed, affected some 265 power plants and cost an estimated six billion dollars.[95] If such an incident could result from an accident at one utility, one can only imagine the catastrophe that a well-planned terrorist attack on critical infrastructure would cause.

While some experts insist that defensive measures are the solution to preventing attacks on the eighteen critical infrastructures identified in the U.S. National Infrastructure Protection Plan (2009), in reality, there are not enough resources or time available to secure all of the ever-changing vulnerabilities associated with these systems. Even the most outspoken supporters of protection seek to deal with this reality by incorporating risk management methods to determine how best to distribute the finite amount of resources available for this endeavor. Unsurprisingly, the main argument against this defensive approach simply points out that it is impossible to protect everything. Although protective efforts might deter terrorists from attacking a hardened

[94]Homeland Security Council, *National Strategy for Homeland Security*, 1–53, 25.

[95]Ibid., 11–12.

target, they do not preclude terrorists from exploiting the unprotected soft targets instead.[96] Furthermore, since America arguably has an infinite number of vulnerabilities, attempting to secure all of them would be an ineffective use of national treasure that, in the end, could prove economically disastrous for the nation.[97] These limitations suggest that deterring terrorist attacks by threat of punishment provides a logical supplement to the aforementioned strategy because it can address gaps that will remain—despite the nation's best efforts to secure a limitless number of targets or disrupt covert operations. Therefore, the United States should use the threat of punishment to influence terrorists' will to commit attacks on the nation's critical infrastructure to supplement the limitations of defensive strategies. This reality is no different than the outcome of decisions by leaders faced with a similar dilemma during the nuclear arms race—defense is not an answer unto itself. By establishing an effective and credible message aimed specifically at deterring attacks on U.S. critical infrastructure and key resources, the United States can encourage non-state actors to consider the unacceptable consequences of these types of attacks and choose an alternate course of action to further their goals.

In this chapter, I attempt to determine the likely responses to a cyber attack on U.S. critical infrastructure by a non-state actor and examine the credibility of policy threats related to this scenario. The intent is to evaluate the retaliation options substantiated in chapter two as potential responses to a hypothetical scenario. I will begin with a review of relevant policy documents to discuss the current strategies on deterring this type of terrorism. Through this I will also identify any threats contained within current strategy that would specifically signal U.S. intent to non-state actors contemplating attacks on America's critical infrastructures. Next, I present a realistic scenario that illustrates the events and actors involved in a cyber attack on the United States. The scenario will depict an act of cyber-terrorism on the nation's critical infrastructure by a non-state actor that causes severe damage and significant financial loss. Through analysis of that event, I will derive a list of potential targets for reprisal

[96]Bowen, "Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism," 54–70, 62.

[97]Colby, "Expanded Deterrence: Broadening the Threat of Retaliation," 43–59, 44; Davis and Jenkins, "Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda," 86, xiv.

based on the enablers and culpable actors involved in the attack. Then, I will determine whether these threats are valid responses in light of the consequences of the given attack. And finally, I will compare the methods of punishment validated in chapter two with potential targets derived from the scenario in order to analyze their credibility based on effectiveness and political support. If the threats declared in U.S. policy do not threaten influential targets or would reasonably fail to garner political support, then presumably the threats would lack credibility.

To provide a common frame of reference, the 2006 National Strategy to Combat Terrorism defines critical infrastructure as "systems and assets so vital that their destruction or incapacitation would have a debilitating effect on the security of our Nation."[98] It lists critical infrastructures and key resources as: energy, food and agriculture, water, telecommunications, public health, transportation, the defense industrial base, government facilities, postal and shipping, the chemical industry, emergency services, monuments and icons, information technology, dams, commercial facilities, banking and finance, and nuclear reactors, materials, and waste.[99] While this opens the possibilities to countless scenario options, this study is narrowed to analysis of an attack on the banking and financial sector to illustrate the effects of a catastrophic attack on critical infrastructure without human casualties.

An important component that should be addressed before proceeding is the issue of attribution. Clearly, attribution plays a significant role in any punishment strategy, but cyber-terror attribution may prove extremely difficult, if not impossible. "The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all."[100] Even if the evidence is traced back to a certain computer at a specific location, it still does not prove who was sitting behind keyboard at the time of attack. However, I

---

[98] Executive Office of the President, *National Strategy for Combating Terrorism*, 1–23, 13.

[99] Ibid., 13.

[100] United States Department of Homeland Security, *The National Strategy to Secure Cyberspace* (Washington, D.C.: United States Department of Homeland Security,[2003]), viii.

will assume either successful attribution or that terrorists will claim responsibility for an attack on the premise that some of the benefits of terrorism are lost in anonymity, so as to analyze the relevance of retaliation options.

B. RECENT U.S. POLICY THREATS

This section analyzes the most recent policy documents available at the time of writing. These were mostly released in the second term of the George W. Bush administration, but it is not expected that U.S. strategy for deterring terrorism will change greatly with the new Obama administration. In general, these policies give primary emphasis to the goal of defeating terrorism. Although the preponderance of strategic guidance pertains to methods that seek to prevent and defend against terrorist attacks, the strategies also incorporate statements that signal intent to punish offenders ex post. For example, the 2006 National Security Strategy proposes to cut off radical leaders from their supporting networks and mentions deterring those elements from further collaboration.[101] As a pinnacle document of U.S. strategy, it provides overarching guidance on preventing terrorist attacks and the importance of deterrence, but it lacks any direct reference to the importance of deterring attacks on critical infrastructure.

On the other hand, the 2007 National Strategy for Homeland Security dedicates an entire section to critical infrastructure protection with emphasis on establishing a deterrent posture. Overall, the document's strategy for critical infrastructure focuses on building resiliency and protecting the various components in order to invoke deterrence through denial by reducing the probability of success.[102] However, it does not discard punitive deterrence altogether; rather it points to the limitations when dealing with terrorism. The section addressing punitive deterrence declares the desire to alter the terrorist's calculus and it clearly articulates the intended audiences—state sponsors, terrorist groups, and other non-state actors who support terrorism.[103] Furthermore, it

---

[101] Executive Office of the President, *The National Security Strategy of the United States of America* (Washington: The White House, [2006]), 12.

[102] Homeland Security Council, *National Strategy for Homeland Security*, 1–53, 25–30.

[103] Ibid., 25.

discusses actual methods to retaliate, such as alienating supporters, prosecuting terrorists, launching counter-narrative campaigns, and pursuing global engagement.[104]

It also highlights America's growing vulnerability to cyber attacks and notes that critical infrastructure "relies on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise [its] cyber infrastructure."[105] Cyber infrastructure not only provides a powerful medium to help non-state actors conduct their internal operations, it also provides a conduit for terrorists, criminal hackers, and foreign governments alike to globally attack a nation's economy, its citizens, and its defense systems. A severe cyber-terrorism attack could seriously impact the "highly interdependent" critical infrastructure systems, thereby weakening the national economy and security.[106]

Two additional policy documents directly address the topic of critical infrastructure protection initiatives of the Homeland Security strategy: the 2003 National Strategy to Secure Cyberspace and the 2003 National Strategy for the Physical Protection of Critical Infrastructure. The Cyberspace strategy document provides details on specific vulnerabilities and guidance on protective measures to prevent attacks and mitigate their effects. Also, it also touches on the need to strengthen law enforcement, counterintelligence and attribution capabilities as well as foster international unity against cybercrime.[107] The Physical Security Strategy document primarily focuses on the physical protection of critical infrastructure across the spectrum of public and private sectors. This document also highlights the interdependence of these infrastructure systems by reaffirming that a debilitating attack on one could cascade across multiple systems.[108]

---

[104]Homeland Security Council, *National Strategy for Homeland Security*, 1–53, 27.

[105] Homeland Security Council, *National Strategy for Homeland Security*, 28.

[106] Ibid.

[107] United States Department of Homeland Security, *The National Strategy to Secure Cyberspace*, 1–61, xii–xiii.

[108] Executive Office of the President, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: The White House, [2003]), 81.

Finally, the 2006 National Strategy for Combating Terrorism signals the threats of U.S. response to terrorism (detailed in chapter two) as: attacking ideology; targeting leaders, foot soldiers, propaganda, weapons and communication; disrupting recruitment and material and financial support; and waging a war of ideas through democratization and promoting freedom.[109] Although this document provides the preponderance of specificity on methods to combat terrorists, it does not associate any threat of retaliation distinctively for an attack on critical infrastructure. Instead, it echoes the Department of Homeland Security's reliance on a defensive strategy for protecting U.S. critical infrastructure. Overall, the aforementioned policies lean heavily on protection methods and do not signal specific reprisal for attacks on critical infrastructure. Nonetheless, such attacks would still be characterized as acts of terrorism and therefore would presumably invoke the counterterrorism measures listed in Table 1.

C. CYBER-TERRORISM SCENARIO

The 2003 National Strategy to Secure Cyberspace describes cyberspace as the nervous system of the nation's critical infrastructures.[110] While U.S. critical infrastructure has yet to suffer the level of attack that would warrant a national level deterrence strategy, it is continually subjected to smaller-scale cyber attacks, which expose its vulnerabilities. These attacks have been either criminal in nature or non-destructive probing and data mining by competing nation-states. Nevertheless, while cyber-terrorism has yet to cause severe damage or financial loss, cybercrime currently deprives the U.S. economy of $200 million to a billion or more per year (estimates vary by how financial loss is measured).[111] Regardless of the figure, critical infrastructures such as the financial sector, electrical grid and national defense systems provide lucrative targets with vulnerabilities susceptible to cyber terrorism.

---

[109] Perl, "National Strategy for Combating Terrorism: Background and Issues for Congress," 1–16, 5–8.

[110] United States Department of Homeland Security, *The National Strategy to Secure Cyberspace*, 1–61, vii.

[111] T. G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, N.J.: Wiley-Interscience, 2006), 474, 244; Ibid., 399.

The 2004 National Planning Scenarios, developed by the Homeland Security Council and Homeland Security Department, describe potential disasters that would cause catastrophic damage to the United States. Within this document's fifteen national emergencies is a realistic scenario in which a non-state actor attacks the nation's critical infrastructure. In this scenario, a non-state actor uses a clandestine computer network from outside the country to conduct a cyber-based attack on critical infrastructure accessible through the global Internet.[112] The scenario demonstrates how a cyber attack on the financial sector can undermine confidence in the nation's banking system, resulting in severe economic disruption and financial damages.

The scenario begins with leaders of a non-state organization strategizing to commit cyber terrorism on the financial sector in order to severely degrade the national economy. The terrorist leaders assemble a team of computer hackers to develop an operational plan to infiltrate and exploit the main computer databases of major credit card companies. Their primary target is the credit-card processing facilities, which are highly interconnected with the U.S. banking system.

To set the plan in motion, the terrorists establish a network operations center in a location permissive to cybercrime, in other words, where unmonitored financial transfers and unregulated communications are possible. Financial and material supporters provide the necessary computer equipment, communications links, and funding to establish a powerful computer network. From this location, the hackers begin a long period of undetected and non-destructive attacks on the targeted systems in order to determine vulnerabilities, which are then exploited by planting malicious code that will perform a specific function at the prescribed time. Simultaneously, the team constructs an encrypted attack network consisting of thousands of bots (innocent zombie computers on the network) that are populated with undetectable software. This attack network will be used to shut-down Internet hubs that interconnect the bank's computer systems to further disrupt service and degrade response capabilities.

---

[112] United States Department of Homeland Security, *National Planning Scenarios: Executive Summary* (Washington D.C.: United States Department of Homeland Security, [2004]), http://www.ccroa.org/index.php (accessed 8/08/2009), 15–1.

When everything is in place and ready, the leaders decide to execute the plan on the eve of Thanksgiving—hours before the biggest shopping day of the year, Black Friday. During the attack, terrorists steal credit card numbers from multiple credit-card processing facilities and post them on the Internet. This causes the cancellation of 20 million cards that unsuspecting people intend to innocently use the next morning. A daisy chain of events causes automated tellers to shut down across the country, payroll systems of large corporations to fail, and major investment management companies to shutdown. As a result, "citizens no longer trust any part of the U.S. financial system and foreign speculators make a run on the dollar." [113] All of which causes the U.S. economy to fall into a long-term crisis. While this may sound like a science fiction, the reality of this type of attack was confirmed in 2007 when Chinese cyber spies stole a significant amount of defense research and development data from the computer systems of a U.S. company through a very similar process.[114]

D. POTENTIAL TARGETS OF RETALIATION

Analysis of this attack yields fewer targets for retaliation than would a mass-casualty bombing because it requires a smaller number of operatives, limited transnational travel and less logistical support. Nevertheless, members of the terrorist network (leaders and foot soldiers) are potential targets of retribution. In this case

---

[113] United States Department of Homeland Security, *National Planning Scenarios: Executive Summary*, 15-1.

[114] Siobahn Gorman, "China Expands Cyberspying in U.S., Report Says," *Wall Street Journal*, sec. Technology, October 23, 2009, 2009, http://online.wsj.com/article/SB125616872684400273.html (accessed 10/23/2009). "In the months leading up to the 2007 operation, cyberspies did extensive reconnaissance, identifying which employee computer accounts they wanted to hijack and which files they wanted to steal. They obtained credentials for dozens of employee accounts, which they accessed nearly 150 times. The cyberspies then reached into the company's networks using the same type of program help-desk administrators use to remotely access computers. The hackers copied and transferred files to seven servers hosting the company's email system, which were capable of processing large amounts of data quickly. Once they moved the data to the email servers, the intruders renamed the stolen files to blend in with the other files on the system and compressed and encrypted the files for export. Before exporting the data, the collection team used employee accounts to take over four desktop computers to direct the final stage of the operation. They selected at least eight U.S. computers outside the company, including two at unidentified universities, as a drop point for the stolen data before sending it overseas. The high Internet traffic volume on university networks provides excellent cover. The spies activated the operation on all seven servers almost simultaneously, which suggested a plan to export the data as quickly as possible. The company's computer-security team eventually detected the outflow of data, but 'not before significant amounts of the company's data left the network,' according to the report."

specifically, the attack is carried out by computer hackers who are most likely culpable actors, but could include a few unwitting cyber criminals that performed a small function in the larger plan. Regardless, they would still warrant punishment as terrorist supporters if not active members. Financial and material supporters both legitimate and criminal provide additional targets for retribution efforts. These would include legitimate companies and institutions that knowingly do business with terrorists and criminal organizations that supply weapons and materials on the black-market. The command and control system, especially the communications network and facilities enabling the attack, provides the only hard targets for retaliation. As with most terrorist groups, the strategic goals of the organization are susceptible to attacks that counter those goals and derail their political agenda. Lastly, community and state supporters enable the non-state actor to operate with impunity by providing a location from which to base its operations and covertly commit a cyber-attack. These targets comprise the retaliation options that would be most effective for this type of attack.

E. EVALUATION OF POSSIBLE RESPONSES

In order to determine the effectiveness of the policy threats validated as relevant forms of retaliation in chapter two, they are compared to the list of targets from the analysis above. To recall, the policy threats were extracted from the counterterrorism strategies found in the national strategy documents of the United States. These policy threats are evaluated in the context of this scenario to determine their credibility as a response to a cyber attack on critical infrastructure.

Since this attack might lead to hundreds of millions of dollars in immediate financial loss and send the nation's economy into a depression, public support for a national response is almost certainly garnered. However, the outcry for justice would not compare to that in reaction to the attacks on 9/11. The nation would undoubtedly wage a war of ideas by countering the terrorist's ideology and propaganda while also seeking to discredit the organization and its leaders. The U.S. could launch an all out information campaign that promotes counter-narratives and exposes the negative aspects of the terrorist organization. The battleground would include any region in which the

organization seeks to influence local communities, and include a global engagement strategy that seeks to dominate information sources on the Internet.

Also, there would be little resistance to hunting down the terrorist leaders and operatives directly responsible for the attack, but it is highly unlikely that Americans would support a "kill or capture" policy for an act of cyber terrorism that does not directly cause casualties when one considers that there is opposition to the death penalty for criminals convicted of murder. In the same sense, killing terrorists for non-lethal crimes would not correlate to the American sense of moral justice. Considering this caveat would, theoretically, eliminate any retaliation option that targets individuals with lethal methods for this scenario. The more realistic form of punishment for complicit individuals would be a transnational law-enforcement operation to bring them to justice. Additionally, the U.S. would seek retribution against the financial supporters and systems that contributed to the attack. For example, the U.S. could expose and discredit any charities and businesses that support the group as well as prosecute those complicit in the attack. It could also seize any existing financial resources connected to the organization and pursue financial investors for reparations.

Another threat to evaluate for this scenario is retaliation against non-state supporters, or counter-societal targeting. In this case, punishing the community that is providing a hospitable environment or providing popular support presents some complications. The U.S. could cut off aid or impose economic penalties on the local community and law enforcement could pursue complicit individuals from that community. However, any benefit gained from punishing the community at large would not offset the audience costs of targeting "innocent" civilians in retaliation for monetary damages alone. Moreover, it is difficult to imagine that the American people would support any form of retaliation that involved taking human lives in response to an attack that only inflicted financial havoc on America.

The scenario does illustrate how state support can contribute to a successful attack by providing a permissive environment for cyber crime and safe haven for terrorist organizations. However, attacking every safe haven could prove difficult for cases of

cyber-terrorism because terrorist hackers can use virtual safe havens which are not geographically bound to each other or the terrorist network.[115] Also, gaining consensus to punish the supporting nation-state by forcing a regime change would be more challenging than it would in response to a more graphic attack that inflicted severe damage and mass casualties. A cyber attack of this magnitude might bring together international support for economic sanctions aimed at forcing the guilty state to strengthen its cyber laws and enforcement measures. However, considering the opposition America faces when seeking sanctions against nuclear-proliferation violators and rogue states (e.g., Russian and Chinese resistance to sanctions on Iran and North Korea), convincing the international community to pass sanctions for a cyber-attack poses uncertainties that further reduce the threat's credibility.

The least contentious targets and most susceptible to military strikes are the communications networks and platforms enabling the attack as well as the terrorists' command and control facilities. First, retaliation against terrorist facilities aligns quite well with the U.S. military's capabilities, and would represent a direct attack on the terrorists' capabilities. On the other hand, communication systems involved in this attack start at the terrorists' lair but end at the U.S. cyber infrastructure. In response to this scenario, targeting of communications would be limited to the facilities and systems of the supporting state because it afforded the permissive environment to infiltrate the global network. Retaliation against communications could come in the form of state isolation (blocking all cyber traffic from that nation) or physical attacks on its communications infrastructure. While the second could be accomplished by various means, it opens the door for one possible use of nuclear weapons in retaliation for cyber terrorism.

Obviously, with this type of attack, the U.S. would not resort to nuclear retaliation against the state or community supporters in the direct sense. But, the U.S. could feasibly detonate a nuclear weapon at high altitude to create an electromagnetic pulse (EMP) that would destroy all electronic devices in the geographical region where the attack originated. Given the reluctance of international norm-abiding nations to break the

[115] Executive Office of the President, *National Strategy for Combating Terrorism*, 1–23, 17.

nuclear taboo, this method of destroying the enemy's cyber capabilities, while realistically effective, would meet political resistance. Therefore, the use of nuclear weapons for EMP strikes would require additional research and analysis before definitively adding it to the list of viable retaliation options.

For simplicity, the results of this comparison are summarized in Table 2: The current counterterrorism policy method (threat) is considered relevant if it correlates with a potential target from the scenario, and credible if it is a plausible response to this type of attack.

Recent U.S. Policy Options	Cyber Scenario Targets	Relevant ?	Evaluation of Policy Threats for Cyber Scenario	Credible ?
Battle of ideas/Democracy	Political goals, propaganda, and recruiting	Yes	Information operations campaign	Yes
Target terrorist network	Leaders, members, hackers	Yes	Kill or capture terrorists, sever links, restrict travel	No*
Target finance	Financiers, charities, businesses, communities	Yes	Seize assets, shutdown charities, seek financial reparations	Yes
Target communications	Command and control system	Yes	Disrupt communications capabilities	Yes
Deny weapons	Computer and network systems	Yes	Target terrorist network capabilities	Yes
Target state sponsor	Permissive state	Yes	Seek regime change/sanctions for cyber attack	No
Target safe havens	Base of operations, network control center	Yes	Military strikes	Yes
Nuclear retaliation	Permissive state	Yes	Nuclear retaliation (EMP may be an alternative option)	No**

* Public would not support a kill or capture policy for an attack the only causes infrastructure and monetary damage
** While this type of attack would not generate the "national will" to employ nuclear weapons, EMP retaliation is possible

Table 2. Evaluation of U.S. policy in response to cyber terrorism

The first two columns illustrate the correlation between policy objectives and relevant targets for this scenario. It suggests that the punishment methods described in counterterrorism strategy clearly align with potential targets of the terrorist system. The next two columns suggest that not all of the associated threats of retaliation for those U.S. policy targets are credible responses for a cyber attack on the nation's critical infrastructure. As discussed above, suggestions that the United States might respond with overwhelming military force, or especially with nuclear weapons, are not credible deterrent threats for a cyber attack on critical infrastructure.

F. CONCLUSION

In practice, the retaliation methods for an act of cyber terror would obviously pale in comparison to the response for the 9/11 attacks by al Qaeda. Therefore, one could reasonably assume that the U.S. would implement a less significant response. While some of the current threats appear plausible in retaliation for a cyber attack (e.g., terrorists, finance, and communications), the analysis suggests that the U.S. cannot credibly threaten all of the targets described in recent policy. Although these threats would not be reasonable responses to this scenario, current policy does not differentiate retaliatory options by type of attack. It signals the intent to punish all acts of terrorism by pursuing all of the aforementioned counterterrorism measures against all of the targets identified.

A United States response to this scenario would most likely embrace measures that focus retaliatory efforts at the terrorist system and the cyber network enabling the attack. Attacking the terrorist system would include trying to capture all terrorist leaders, members, and direct supporters to bring them before the justice system for punishment. It would also target all sources and channels of financial backing by seeking to arrest those complicit in the attack, seize funds for reparations, and shutdown guilty businesses and charities. Finally, the communications systems, hardware, facilities, and networks involved in the attack would be disabled or destroyed in order to not only prevent future attacks, but to punish permissive states and companies that fail to police their systems.

However, the response would most likely exclude a policy to kill terrorists, use the military to force regime change, or impose counter-societal targeting as methods of punishment for this type of attack. For example, there would be resistance to a "kill or capture" strategy for punishing terrorists. Depending on the type of attack this threat lacks credibility—it may be effective for a 9/11 type attack, but not for a cyber attack. The same case can be made with state-level retaliation, where regime change may be an extreme punishment for cyber-terror, but support for a domestic opposition's peaceful bid for power would not. Finally, community support provides a potential target in this scenario, but the method of punishment in policy is unclear and could be interpreted to signal counter-societal targeting rather than a lesser form of punishment such as severing financial aid.

This suggests that some punishment measures are too vaguely threatened or directed at general targets, and therefore incredible forms of retaliation. Just as criminal law assigns a degree of punishment based on the type of crime and consequence, deterrent threats must clearly articulate the associated punishment to the type of attack. Therefore, threats against these targets would have to include more specificity about the methods of punishment to be credible.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EVALUATION OF RESPONSES FOR A NUCLEAR ATTACK

A. INTRODUCTION

Anders Corr claims that with a probability of nearly 50 percent over the next ten years, nuclear terror poses a threat with 100 times more destructive potential than Pearl Harbor and 9/11 combined.[116] By establishing a sound and credible deterrent policy the United States can articulate the costs it would impose after such an attack on non-state actors and states that support them, in the hope of dissuading them from attempting such an attack. More importantly, when considering the United States' responses to previous attacks on American soil, it appears likely that the U.S. response to a nuclear attack would be both formidable and inevitable. Hence, not devising a credible threat policy for deterrence would waste the ex ante benefits of an ex post reality.[117] This raises two important questions: what threats does current U.S. strategy signal to non-state actors contemplating nuclear terror and are they credible?

Through a qualitative process I attempt to examine these questions and determine the likely responses to a nuclear attack on the United States. First, I will review existing policy to explore the current strategies on deterring nuclear terrorism. Next, I present a hypothetical scenario to illustrate a conceivable nuclear attack on the United States by a non-state actor. The scenario will illustrate an attack in which a transnational organization manages to acquire or construct a nuclear bomb which is then detonated within the United States resulting in mass destruction and significant casualties. Through analysis of the event, I will derive a list of relevant retribution targets based on the enablers and culpable actors involved in the attack. Next, I will discuss the methods of punishment described in counterterrorism policy, then analyze their effectiveness and practicality based on the relevant targets derived from the scenario and expected public

[116]Anders Corr, "Deterrence of Nuclear Terror," *The Nonproliferation Review* 12, no. 1 (2005), 127, http://www.informaworld.com/10.1080/10736700500208876 (accessed 4/21/2009), 127.

[117]Ibid., 129.

support. Finally, the results are tabulated in order to compare them to the results from the critical infrastructure attack scenario of Chapter III.

B. ASSUMPTIONS

The question that immediately comes to the forefront of this discussion is whether the United States would use nuclear weapons in retaliation for an act of nuclear terrorism. No question, the nuclear arsenal currently supports America's strategic deterrence policy to prevent other nation-states from threatening its sovereignty and plays a significant role in extended deterrence for its allies, but it is unclear if the use of nuclear weapons would be a realistic option for response to an attack by a non-state actor. As Paul Kapur suggests, nuclear retaliation in response to a nuclear attack on the United States is entirely plausible, when considering its Cold War policy to launch nuclear attacks on the Soviet Union for a conventional attack on Europe.[118] However, the Soviet Union was a nation-state with a government responsible for acting on behalf of its citizens, making counter-societal targeting seemingly more justifiable than a situation with non-state actors and dispersed supporters. Stephen Younger claims that nuclear weapons serve only to deter states and present an ineffective tool for deterring non-state actors.[119] A significant amount of literature debates its plausibility, but most experts agree that even for an act of nuclear terror, nuclear retaliation would be limited to punishment of states if they were complicit in the attack. This question is revisited after discussion of a nuclear attack scenario in the analysis of probable U.S. response options.

However, an important component that should be addressed before proceeding is the issue of attribution. Clearly, attribution plays a significant role in any punishment strategy, but even more so when considering the possible response to a nuclear attack. For the victim to deliver true justice, the guilty party must be identified before it can be punished. The United States would have to be able to determine the source of nuclear material and the liable actors to respond with large-scale conventional retaliation or

[118]Kapur, *Deterring Nuclear Terrorists*, 124.

[119]Younger, *The Bomb: A New History*, 238, 208.

nuclear weapons against societal targets. Several U.S. policy documents recognize this issue, stating that America must "refine the ability to define the nature, source, and perpetrator of an attack" and "ensure that our capacity to determine the source of any attack is well-known, and that our determination to respond overwhelmingly to any attack is never in doubt."[120] Michael Miller calls for improvements to nuclear attribution, stating that successful attribution in itself creates a deterrent effect because it removes the terrorists' and supporters' anonymity.[121] The National Strategy to Combat Weapons of Mass Destruction echoes these points and establishes policy initiatives to field new capabilities for rapid attribution and robust strike capability.[122] Here, I will hold this variable constant by assuming that either attribution will be possible after an attack or terrorists will claim responsibility so as to maximize the benefits of their attack.

Additionally, this discussion assumes that terrorists possess the will and potential to obtain nuclear weapons, and simply postulates that an effective deterrent strategy aims to dissuade terrorists that have a desire for acquisition. The first part of this assumption is founded on declaratory statements from terrorist organizations like al Qaeda and recorded attempts by Aum Shinrikyo to obtain and use Weapons of Mass Destruction (WMD) technology, but the second premise involves the more widely-debated issue of *access*. The difficulty in acquiring protected WMD materials and technology provides an opportunity for external influences to attack the supply-side of proliferation.

Counter-proliferation strategies attempt to prevent an attack by employing a strategy of deterrence by denial that seeks to deny terrorists the means to acquire WMD, regardless of their will to possess. For example, Auerswald claims that preventing WMD transfer remains the most important goal and suggests implementing a denial strategy aimed at transnational criminal organizations and traffickers under an international law

[120]Homeland Security Council, *National Strategy for Homeland Security*, 1–53, 27; Executive Office of the President, *National Strategy for Combating Terrorism*, 1–23, 14.

[121]Michael Miller, "Nuclear Attribution as Deterrence," *Nonproliferation Review* 14, no. 1 (2007), 33–60, 42.

[122] Executive Office of the President, *National Strategy to Combat Weapons of Mass Destruction* (Washington, D.C: The White House, [2002]), 3.

framework.[123] In other words, a counter-proliferation strategy attempts to control the supply of WMD materials. In contrast, a punishment strategy seeks to influence and manipulate the demand side of the WMD transfer process by reducing the desire for these weapons. Colby argues that WMD proliferation is inevitable and trying to prevent it a waste of resources, therefore deterring attacks remains the preeminent strategy that, if effective, would reduce incentive for acquiring WMD.[124] Although counter-proliferation is neither completely effective against nor directly targeted at non-state actors, nevertheless it remains an important part of a comprehensive national security strategy. Moreover, Kapur provides an analysis of both supply and demand requirements of nuclear terrorism and concludes that states can pursue both as they are not mutually exclusive.[125] Therefore, if the potential for proliferation exists, then creating a strategy that reduces demand for WMD only serves to bolster counter-proliferation efforts and should be pursued.

C. RECENT U.S. POLICY THREATS

As with Chapter III, this section analyzes the most recent documents available at the time of writing. Also, the U.S. strategy relating to deterring WMD terrorism on the United States is not expected to change drastically with the Obama administration. The first document reviewed, the 2006 National Security Strategy, focuses on counter-proliferation and deterrence by denial methods while declaring that U.S. strategy does not rely on threat of punishment.[126] Instead, this strategy builds on denying enemy objectives and reserves retaliation for events of policy failure. More importantly, it establishes two target audiences (terrorists and source states) through its statement that "terrorists continue to pursue WMD and that some of the world's weapons-grade fissile material is not properly protected."[127]

---

[123]Auerswald, "Deterring Nonstate WMD Attacks," 543–568, 567.

[124] Colby, "Restoring Deterrence," 413–428, 427.

[125]Kapur, *Deterring Nuclear Terrorists*, 122.

[126] Executive Office of the President, *The National Security Strategy of the United States of America*, 49, 18–22.

[127] Ibid., 19.

Likewise, the 2007 National Strategy for Homeland Security echoes the claim that terrorists intend to acquire WMD to carry out massive attacks on America.[128] Maintaining consistency with the previous document, it also promotes deterrence by denial methods, but incorporates a more robust punishment strategy. The policy also provides more specificity on the intended targets of threat: state sponsors, terrorist groups, and other non-state actors who support terrorism.[129] Furthermore, it discusses actual methods to retaliate such as alienating supporters, prosecuting terrorists, counter-narrative campaigns, and global engagement.[130]

The 2006 National Strategy for Combating Terrorism and the Strategy to Combat Weapons of Mass Destruction directly address the issue of nuclear terrorism. The first establishes a "new deterrence calculus" aimed at the demand side of WMD, but leans heavily toward non-punitive forms of deterrence as it claims that terrorists are less responsive to threats. However, the first document vaguely refers to the threat of nuclear retaliation in response to nuclear terror. It states that "terrorists and those who aid or sponsor a WMD attack would face the prospect of an overwhelming response to any use of such weapons."[131]

Likewise, the 2002 National Strategy to Combat Weapons of Mass Destruction declares the "right to respond with overwhelming force—including through resort to all of our options—to the use of WMD against the United States, our forces abroad, and friends and allies."[132] As Freedman describes it, this policy brings together multiple concepts to form a new deterrence strategy that combines arms control, active defenses, and preemptive action with threat of punishment as the foundation.[133] Furthermore, through this document the U.S. signals a more direct punishment message to states with

---

[128] Homeland Security Council, *National Strategy for Homeland Security*, 1–53, 6.

[129] Homeland Security Council, *National Strategy for Homeland Security*, 25.

[130] Ibid., 27.

[131] Executive Office of the President, *National Strategy for Combating Terrorism*, 1–23, 14.

[132] Executive Office of the President, *National Strategy to Combat Weapons of Mass Destruction*, 3.

[133] Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan, 2003), 566, 453.

nuclear technology and material. It threatens to destroy the "residual WMD capabilities" for a nuclear attack and reaffirms that such a response will deter others from pursuing such weapons.[134]

D. NUCLEAR TERRORISM SCENARIO

Although terrorists have conducted small-scale WMD attacks using sarin gas and anthrax, to date they have not executed an act of nuclear terror. While this undoubtedly is a welcomed reality, it does limit the research material available for establishing a historically-rooted attack scenario. And, unfortunately, some of the best sources for hypothetical illustrations are found in fiction novels. Regardless, there are two ways this type of attack could occur: Either a non-state actor acquires or builds a nuclear device by criminal means, or a state willingly provides an intact weapon. Taking these divergent paths into consideration, retaliation options would have to include measures to address each case.

However, as Whiteneck argues, stateless nuclear terrorism is more likely, because states understand that they are easier to punish and so realize the weakness of relying on anonymity.[135] Also, state-supported nuclear terror would constitute an act of war by a nation-state, which more aligns with traditional national security strategy. Therefore, the most relevant scenario for evaluating U.S. response to nuclear terror would depict a non-state actor acquiring a nuclear device or fissile material *without* deliberate state support. One such scenario is found in the 2005 National Planning Scenarios developed by the Department of Homeland Security, which describes the background information and predicted effects of a ten kiloton improvised nuclear device detonating in Washington, D.C.

---

[134] Executive Office of the President, *National Strategy to Combat Weapons of Mass Destruction,* 3.

[135] Whiteneck, "Deterring Terrorists: Thoughts on a Framework," 187–199, 193.

In this scenario, highly enriched uranium is stolen from stockpiles in Russia then sold on the black market to a non-state actor for a significant amount of money.[136] The material is smuggled to a third country where the terrorists have safe haven and have built an underground laboratory. There, a couple of scientists use the HEU to build a gun-type nuclear weapon with a potential yield of ten kilotons. The terrorist leaders devise a plan to have operatives, with the help of other supporters, detonate the weapon in a U.S. city. The non-state actor uses sympathetic businesses to ship two sets of the weapon's non-nuclear components to America. Also, a senior lieutenant of the organization with assistance from criminal elements smuggles the fissile material across the border and is met by supporters already in the America. Those supporters provide a safe house, transportation and supplies to the bombers. Once everything is in place, the leaders provide the bombers with a time and place to detonate the weapon—the center of Washington, D.C., on a busy weekday.

The immediate blast and fire effects coupled with secondary effects result in significant casualties and damage. The immediate damage to infrastructure reaches out to nearly a kilometer in every direction with eventual contamination covering approximately 8,000 square kilometers. The electromagnetic pulse generated by the detonation has effects as far away as five kilometers. The population receives several blows beginning with the blast overpressure, fragmentation, extreme heat, and gamma radiation exposure from the initial explosion, then radiation sickness from subsequent effects of radioactive fallout, and so on. The scenario estimates over 70,000 fatalities and more than 600,000 injured at the onset with those numbers continuing to grow for several days thereafter (see Appendix for more details). Also, those who are not seriously injured must evacuate the contaminated area resulting in the displacement of another million persons. Finally, the economic impact resulting from all of this would cost the nation hundreds of billions of dollars.[137]

---

[136] United States Department of Homeland Security, *National Planning Scenarios* (Washington D.C.: United States Department of Homeland Security, [2005]), http://www.ccroa.org/index.php (accessed 8/08/2009), 1.1–1.2.

[137] United States Department of Homeland Security, *National Planning Scenarios*, 1.1.

E. POTENTIAL TARGETS OF RETALIATION

From the scenario described above, one can quickly extract the fundamental actors involved with successfully acquiring and detonating an improvised nuclear device on American soil. It is clear that the organization's desire alone will not deliver a nuclear weapon, but rather it requires a significant amount of capital and a source of nuclear materials. Additionally, a common component to either stealing a weapon or the fissile materials to build one is the involvement of international criminal networks for acquisition and smuggling operations. Auerswald notes that literature on crime and deterrence supports targeting criminals that traffic weapons of mass destruction because these elements are not ideological zealots and tend to pursue crimes with high ratios of payoff to risk.[138]

Furthermore, the terrorist network (its leaders and members) provides the intent and pursues the means, but bringing desires to fruition are the scientists, businesses, and community supporters. Also, safe communications for effective command and control enable operations from the acquisition of nuclear material to the successful detonation. Analyzing the state-support aspect of this scenario provides two prospects. First, the state failing to secure nuclear materials bears some responsibility, regardless of its intentions. The second state-level target for this scenario is the one providing the terrorists safe haven from which to base operations and operate the weapons laboratory. The punishment options for each state will likely be affected by the degree of negligence and extent of knowledge.

The next step is to determine the list of relevant threats found in current policy documents. Recalling the policy analysis from Chapter II, current counterterrorism strategies found in the National Strategy for Combating Terrorism and the Strategy to Combat Weapons of Mass Destruction provide methods that the United States intends to employ against terrorists. Its counterterrorism measures target the following components: ideology, propaganda, terrorist network, funding, means-of-travel and

[138]Auerswald, "Deterring Nonstate WMD Attacks," 543–568, 556–558.

communication, state support, and safe havens. While these strategies are clearly directed at a vulnerability of the terrorist network, the specific WMD policy which refers to responding with nuclear weapons instead signals a particular method of retaliation without reference to the target. Nevertheless, it does reveal the threat of nuclear retaliation in response to a WMD attack on the United States by a non-state actor. Therefore, nuclear retaliation has been included with the other forms or retaliation to formulate a list of threats signaled by current U.S. policy in response to a terrorist attack.

F. EVALUATION OF POSSIBLE RESPONSES

Reflecting on the response to 9/11, the American people would support the majority of reprisal options described above. Beginning with the terrorists' political goals, America would launch an all out counter-narrative and military campaign against those aims while providing unprecedented support to the terrorists' opposition. It would also destroy or disrupt the terrorists' communications capabilities while launching a full cyber-warfare campaign to shutdown their ability to exploit the Internet. Those regions providing fertile populations for radicalization would be targeted with unprecedented non-kinetic nation building and democratization operations. The United States would pursue the entire organization and affiliated networks with more prowess and persistence then it did with al Qaeda after 9/11. Setting out to kill or capture the terrorist leaders and those involved in the nuclear attack would most likely be demanded, not just accepted. Non-state supporters that supply materials, access to business operations, and provide safe houses and transportation would be globally pursued and prosecuted by various means and methods to include military operations.

Without question, the nation would support global seizure of funds and assets from those that provided material and financial services to the terrorist organization as reparations. Any business or charity organizations found guilty of providing support to the non-state actor would be attacked by the various elements of national power to inflict severe defamation and degrade their ability to continue operating. Also, the United States would manipulate foreign aid and pursue economic sanctions to retaliate against supporting communities of any nation.

In order to deny the terrorist any capability for future attacks, the Unites States would use whatever means necessary to destroy residual weapons capabilities to include targeting those criminal elements which provided the nuclear materials. It would globally pursue the suppliers, arms dealers, smugglers, and their organizational affiliates in order to bring them to justice. Whether the host nation government willingly provided a permissive environment or simply turned a blind eye, it could expect the United States to force a regime change or support an opposing movement's bid for power. This effort would run congruent to efforts that target the terrorists' base of operations, training camps, weapons laboratories and other facilities within the host nation. However, it is reasonable to assume that the level of retaliation directed towards the supporting state would be proportional to that state's material power and culpability in the attack.

As a matter of fact, there would be little debate about fully implementing all retaliatory strategies of recent policy until considering punishment against another nuclear-power state and, more controversial, whether that reprisal would incorporate nuclear weapons. While it is clear the United States would pursue the criminal elements involved in supplying fissile material, direct retaliation against Russia seems unlikely in this scenario. For example, it could target Russia's apparently unsecure stockpiles of residual nuclear materials, but military strikes increase the risk of escalating war with a nuclear-armed adversary. Clearly, the target nation's second-strike capability will affect the decision to retaliate with nuclear weapons regardless of culpability. Not only could Russia retaliate in kind, it could also claim to have made a real effort to secure nuclear materials due to its willingness to accept U.S. assistance in dismantling and securing its nuclear arsenal. As part of this assistance, the U.S. has spent hundreds of millions through the Cooperative Threat Reduction program and billions more to purchase HEU under the "Megatons to Megawatts" agreement.[139]

Furthermore, one could reasonably question whether the American public would support the use of nuclear weapons on societal targets of a nation that provided the

[139]Stephen I. Schwartz, *Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons since 1940* (Washington, D.C.: Brookings Institution Press, 1998), 680, 345–346.

terrorists safe haven or supported the terrorist network because most of the population might be non-complicit third-parties. Although, after an attack, some part of the U.S. public would likely be unconcerned with this distinction in its desire for vengeance, it would be hard for the United States to openly threaten nuclear annihilation of innocent civilians ahead of time. Even if the terrorists claimed responsibility for nuclear terror, thereby removing any doubt concerning attribution, identifying a viable target that would garner political support for a nuclear strike remains difficult. In other words, since terrorists have no national territory to threaten, nuclear retaliation is realistically limited to (but not required for) state-sanctioned nuclear terrorism.[140] Furthermore, opponents of nuclear retaliation would claim that conventional military ordnance provides sufficient capability for punishing or destroying the more localized terrorist targets and third party supporters as well as residual WMD stockpiles. They would also argue that a nuclear strike that killed innocent civilians would cause the United States to lose world sympathy and the moral high ground and would generate new support for the terrorists.

This brings us back to the question of whether the U.S. could credibly threaten to employ nuclear weapons to strike any of these targets. In response to the situation and actors of this scenario, it is hard to support an argument that nuclear retaliation would be employed against Russia for inadvertently "supplying" fissile material as suggested above. But what if it had been a nation without a (nuclear) second-strike capability such as North Korea, Pakistan, or Iran? If everything stayed constant in this scenario except the source state was North Korea, then the United States could launch a nuclear strike without fear of second strike. However, it is not *guaranteed* that political will would support this option if the rogue state was an unwilling victim of crime as in the case of Russia in this scenario. Otherwise, the argument returns to the assumption made earlier that a rogue state willingly providing nuclear capabilities to terrorists would be committing an act of nuclear war for which the United States would be justified in launching a nuclear retaliation (legitimate purpose of America's second-strike capability).

[140] William J. Perry, Charles D. Ferguson and Brent Scowcroft, *U.S. Nuclear Weapons Policy*, Council on Foreign Relations, [2009]), http://www.cfr.org/content/publications/attachments/Nuclear_Weapons_TFR62.pdf (accessed 9/10/2009), 8.

In such a situation, national will and target opportunities would align for a politically acceptable and executable nuclear retaliation option.

An initial "willingness" or even active demand of the American public to use nuclear weapons in response to an act of nuclear terror is certainly conceivable. However, because attributing responsibility for being the source of nuclear materials takes time, the issues associated with threatening unwitting states will likely deflate that "willingness" during the attribution and target selection phase for retaliation. It is reasonable to *doubt* a pledge of nuclear retaliation as a response for this scenario, and it therefore lacks credibility as a threat for deterring stateless-nuclear terror. To summarize the results, the analysis of relevancy and credibility for each threat is illustrated in Table 3. The recent policy threat (counterterrorism strategy) is considered relevant if it correlates to a potential target from the scenario and credible if the retaliation option is a plausible response to the given scenario.

Recent U.S. Policy Options	Nuclear Scenario Targets	Relevant ?	Evaluation of Threats for Nuclear Scenario	Credible ?
Battle of ideas/Democracy	Political goals, propaganda, and recruiting	Yes	Information operations campaign and democratization	Yes
Target terrorist network	Leaders, members, recruiters	Yes	Kill or capture	Yes
Target finance	Financiers, charities, businesses, communities	Yes	Seize assets, shutdown charities, seek financial reparations	Yes
Target communications	Command and control system	Yes	Disrupt communications capabilities, cyber warfare	Yes
Deny weapons	Fissile material stockpile, arms dealers, smugglers	Yes	Destroy residual capabilities and target criminal elements	Yes
Target state sponsor	Permissive state, source of nuclear materials	Yes	Economic sanctions, regime change, reparations, and conventional military engagement	Yes*
Target safe havens	Base of operations and labs	Yes	Military strikes, economic sanctions, regime change	Yes
Nuclear retaliation	Permissive state, source of nuclear materials	Yes	Launch nuclear strike against complicit states	No**

* Retaliation proportional to the state's power and culpability in the attack which could affect credibility
** While "national will" is conceivable, lack of culpability and second-strike capability of states in this scenario raise doubt

Table 3. Evaluation of U.S. policy in response to nuclear terrorism

G. CONCLUSION

The results of this analysis suggest that retaliation methods for an act of nuclear terror would reflect U.S. responses to the 9/11 attacks by al Qaeda. Yet, as devastating as it was, 9/11 would pale in comparison to the scenario described above. Therefore, one could reasonably assume that the United States would seek to punish every target that aligns with striking the influential nodes described above: the terrorist network, its political aims, its finances, its communications, and the supporting state. Also, the analysis confirms that current U.S. policy does contain effective threats to develop a credible WMD deterrence message as evident in the correlation between the main components of the scenario and counterterrorism strategies.

However, some threats are situation dependent or not plausible forms of retaliation, and thus lack credibility. For example, the U.S. could easily threaten a rogue state for supporting terrorists when it possesses overwhelming military superiority, but would that threat remain credible against a country with second-strike capability for nuclear proliferation violations (intentional or inadvertent)? Clearly, targeting the state from which nuclear materials originate poses a dilemma that needs to be discussed in greater detail to establish a universally applicable form of punishment. Nonetheless, effectively deterring non-state actors from committing WMD attacks would eliminate the demand for these materials which alleviates the predicament of punishing Russia or any other nuclear-armed state for allowing WMD to leak to non-state actors. This point highlights the need to make deterring the terrorist network as effective as possible to overcome the difficulty of credibly threatening states that might be sources of nuclear materials. This will require focusing more effort on influencing the demand for WMD.

The evidence also suggests that the U.S. could not sufficiently guarantee that it would retaliate with nuclear weapons if the states involved were not willing participants, but rather victims of a criminal theft or unwitting host to the guilty organization. Therefore, nuclear retaliation would not provide a credible option for responding to

stateless nuclear terrorism. First, targeting states with nuclear retaliation for failing to secure nuclear material would not automatically attain political support. Furthermore, some source nations possess strategic nuclear weapons and therefore have the capability to launch a second-strike on America. Second, it would be very difficult for the United States to target a nuclear strike against a nation that provided safe haven (i.e. where do you aim). Nuclear weapons are indiscriminate and therefore difficult to pinpoint the targeting of guilty parties whether a rogue regime, terrorist camp or community supporters. While nuclear retaliation is not completely unreasonable, these issues do bring into question the surety that it would be employed.

Coincidentally, the research exposed an issue not explored in this study due to its complexity. While the door may not open for nuclear weapons, public tolerance for other measures may relax. For example, under less destructive attacks it would be taboo and inconceivable to establish a deterrent message that threatens to destroy historic or religious places—that might become more plausible in response to an act of nuclear terror. Nevertheless, the important component of threat to signal is the *object* of retaliation and not *how* the target will be attacked. In other words, the legitimacy of targeting a rogue or unwitting state is what limits retaliation options, not necessarily the choice of weapons. If, however, nuclear weapons are to play a role in deterring nuclear terror, the U.S. may need to alter its nuclear strategy and the composition of its nuclear arsenal to achieve the right mix of capabilities.

In closing, a terrorist system requires various components to perform specific operations when mounting different types of attack. Hence, states should direct threat towards those components with the maximum force supported by its population, and that political capital is directly proportional to the level of devastation. Deterrent threats should signal a graduated retaliatory response framework that would align punishment threats with the level of domestic support likely to be generated by the type of attack. Also, an ambiguous threat of nuclear retaliation for an act of terrorism lacks credibility.

Therefore, it should specified as an option for responding to state-sponsored nuclear attacks, but not implicit as a direct threat of punishment for any other nuclear attack. Finally, the results of this analysis provide a sample retaliation framework to create a more direct deterrence message that would clearly articulate the expected punishment for committing a nuclear attack on the United States.

V. CONCLUSION

A. RESULTS

The primary objective of this study was to evaluate the deterrent effect of recent counterterrorism policies of the United States. This objective was accomplished through a two part analysis of the threats to punish terrorist targets found in those policies. The first step sought to validate counterterrorism strategies as *relevant* threats of retaliation for deterring non-state actors. The second step then estimated the *credibility* of those threats deemed relevant by analyzing whether they would be plausible responses to hypothetical attack scenarios. The following sections summarize the results of those evaluations respectively.

1. Validation of U.S. Policy Threats

The results of the first section support the claim that violent non-state actors have goals and assets that, when appropriately threatened, might cause them to make responsive decisions to avoid loss. First, research material on al Qaeda was analyzed to determine how best to depict the behavior of terrorists. This evaluation suggested that non-state actors are organizations and their organizational characteristics come into play when they make decisions. This implies that the deterrer needs to identify and threaten the organizational nodes that influence the decisions and operations of a terrorist system. Therefore, using organizational behavior theory as a lens, the next step was to indentify exploitable vulnerabilities of non-state actors to compare against counterterrorism objectives. For example, non-state actors must maintain key elements of survival: safe havens, anonymity, financial backing, means of travel, and means of communications to name a few.[141] Effectively targeting the vulnerabilities of these nodes should have an effect on the organization's decisions. To that end, the terrorist system model created by Davis and Jenkins was selected to serve as a baseline to evaluate the targets of U.S. policy threats. Consequently, the analysis confirms that punishment methods described

[141] Kean Commission, *9/11 Intelligence Failure*, 417–458, 428–430.

in counterterrorism strategy correlate to vulnerabilities derived from theories on influencing the terrorist system by Davis and Jenkins. This supports the claim that U.S. policy appropriately targets terrorist nodes with *relevant* threats of punishment to influence outcomes.

However, it is important to point out that there are limits to the punishment of those targets based on anticipated U.S. public support. As with any strategy, the nation's population must be willing and able to achieve its objectives. For example, striking a societal target may have a desirable impact on an important center of gravity, but public support could constrain that option, based on how it judges the morality of such reprisal. Therefore, signaling a method of reprisal that does not meet this parameter undermines the credibility of threat and, therefore, fails to meet the prerequisites for deterrence. Just as Americans understood and accepted second-strike policies of the Cold War, the public would have to recognize and assent to the retaliatory threats against terrorism for deterrence to be effective.

2. Credibility of U.S. Policy Threats

Next, the *credibility* of those policy threats deemed relevant in Chapter II was analyzed by comparing the expected responses to two different attack scenarios in Chapters III and IV. The first evaluation determined whether each policy threat would be a plausible response to a cyber attack on the nation's banking system which had caused catastrophic damages to the economy. Then, a similar analysis was conducted to evaluate the expected retaliation for a terrorist attack involving a ten kiloton nuclear detonation in Washington, D.C.

In summary, the analysis in Chapter III demonstrated that while U.S. policy threatens relevant targets for the scenario, it lacks credibility because some of those threats are unrealistic responses to a cyber attack. In practice, the level of retaliation for a cyber attack would pale in comparison to that after the 9/11 attacks by al Qaeda because of the significant difference in human casualties. Therefore, one could reasonably assume that the United States would implement a less significant response. However,

U.S. policy signals the intent to punish all acts of terrorism by pursuing all of the counterterrorism measures and does not distinguish between types of attack or methods of enforcement. And, given that some of the policy threats (e.g., killing terrorists, counter-societal targeting, and nuclear retaliation) appear implausible in response to a cyber attack suggests that U.S. policy does not credibly deter cyber terrorism.

To expound, a United States response to cyber terrorism would most likely embrace measures that focus retaliatory efforts at the terrorist system and the cyber network enabling the attack. Attacking the terrorist system would include capturing all terrorist leaders, members, and direct supporters to bring before the justice system for punishment. But, one could argue that there would be resistance to the "kill" part of the "kill or capture" strategy for punishing the terrorist network. The U.S. response would also target all sources and channels of financial backing to arrest those complicit in the attack, seize funds for reparations, and shutdown guilty businesses and charities. Also, all of the communications systems, cyber hardware, facilities, and networks involved in the attack would be disabled or destroyed in order to prevent future attacks and punish permissive states and companies that fail to police their systems. And yet, the expected retaliation would most likely exclude methods of punishment that employ the use of military forces against either states or societies. For example, even though a host nation had provided a permissive environment for cyber crime, it would be unrealistic to assume the United States would force a regime change or conduct counter-societal targeting in response to an act of cyber terrorism.

Next, the results of Chapter IV suggest that retaliation methods for an act of nuclear terror would at a minimum reflect the U.S. response to 9/11. Yet, as devastating as those attacks were, 9/11 would pale in comparison to the effects of a ten kiloton blast in the heart of a U.S. metropolis. Therefore, one could reasonably assume that the United States would seek to punish every potential target that played a role in the attack: the terrorist network, its political aims, its finances, its communications, its third party supporters, and any supporting states.

This analysis supported the claim that recent U.S. policy does contain effective threats to develop a credible WMD deterrence message as evident in the correlation between the primary targets of the scenario and the targets of counterterrorism strategy. However, some threats are situation dependent or not plausible forms of retaliation, and thus lack credibility. For example, the U.S. could credibly threaten a rogue state for supporting terrorism when the U.S. possesses overwhelming military superiority, but that threat would not be credible against a second-strike-capable nation in retaliation for nuclear proliferation violations (intentional or inadvertent). Therefore, targeting the state from which nuclear materials originate poses a dilemma that needs to be discussed in greater detail to establish a universally applicable form of punishment.

The evidence also suggests that nuclear retaliation would not provide a realistic option for responding to stateless nuclear terrorism. First, targeting states with nuclear retaliation for failing to secure nuclear material would not automatically receive political support. Secondly, as previously mentioned some source nations possess strategic nuclear weapons and therefore have the capability to launch a second-strike on America. Therefore, an ambiguous threat of nuclear retaliation for a terrorist WMD attack may lessen credibility. Instead, policy statements should avoid the implicit threat of nuclear retaliation for any WMD attack and specifically threaten it as a response to *state-sponsored* nuclear attacks. Otherwise the United States would have to change the cultural and international taboos that would undermine public willingness to use nuclear weapons against non-state targets.

3. Summary of Results

The results of this analysis confirm that U.S. policy contains relevant targets and threats for deterring terrorism that evaluated under the two scenarios of this thesis yield different outcomes. The expected response to a cyber attack would clearly differ from that of a nuclear attack, yet U.S. policy declares the same threats for terrorism in general. This is not to say that policy makers lack knowledge or understanding that retaliation will differ based on the attack, but to state that U.S. strategy documents fail to clearly

articulate how responses will differ. Consequently, these undifferentiated signals diminish the potential for counterterrorism strategies to deter non-state actors from committing terrorist attacks on the United States.

The results suggests that a number of punishment measures in U.S. policy are too vaguely threatened, directed at overly general targets, or would be subjected to deliberation before being employed. This uncertainty of punishment reduces credibility of current policy threats because it fails to clearly define the costs of committing acts of terrorism for non-state actors. Just as criminal law assigns a degree of punishment based on the type of crime and consequence, deterrent threats must clearly articulate the associated punishment to the type of attack. The results of these analyses are summarized in Table 4 to illustrate how the general threats of punishment found in counterterrorism strategy documents do not correlate with the retaliation that would reasonably be expected in response to differing attacks.

Recent U.S. Counterterrorism Strategies		Credible Retaliation Threat	
Targets	**Threats**	**Cyber Terrorism**	**Nuclear Terrorism**
Ideology	Battle of ideas (counter-narrative campaign); Democracy (promote rights and freedoms)	Yes	Yes
Terrorist network	Attack terrorist network: kill or capture members	*No*	Yes
Finances	Attack source of funding: seize assets; penalize contributors, charities, businesses; seek reparations	Yes	Yes
Communications	Deny or disrupt communications: stop charity advertisements, sever links, disrupt command and control	Yes	Yes
Weapons and materiel	Conduct military operations, cyber warfare; secure residual WMD materials; go after arms dealers, smugglers	Yes	Yes
State sponsor	Attack the supporting state: economic sanctions, insurgency, military strikes, regime change, counter-societal targeting, seize assets, cut-off aid, restrict travel	*No*	Yes
Safe havens	Destroy all safe havens: physical, cyber, legal, and financial	Yes	Yes
Nuclear retaliation	Use nuclear weapons in response to terrorism	*No*	*No**
* This refers to stateless nuclear terrorism opposed to state-sanctioned nuclear terrorism. Although the U.S. may be willing to use nuclear weapons, a supporting state's lack of culpability or its second-strike capability would introduce doubt on the surety of this punishment.			

Table 4. Mixed credibility of recent policy threats

B. POLICY RECOMMENDATIONS

While U.S. policy does threaten appropriate targets, it also fails to specify what type of punishment would be delivered for a particular attack. Unfortunately, the composition of terrorist systems varies by type of attack because each requires different components to perform specific functions. Hence, the United States should direct threats toward those components with the maximum force supported by its population, and that is likely to be directly proportional to the level of devastation sustained. In other words, deterrent threats should signal a graduated retaliatory response framework that would align with the public willingness to intensify punishment based on the type of attack.

Nevertheless, one could argue that this specificity limits deterrence only to those types of attack identified in policy. However, that would assume the United States does not know precisely what it wants to deter. This does not intend to suggest that calculated ambiguity should be completely abandoned, but rather that it should be incorporated into the sub-level threat messages of an attack-based retaliation strategy. Since it cannot credibly deter all acts of violence with a single threat of retaliation—as shown in the comparison of responses above—the United States should first determine what acts it intends to deter then develop a more defined deterrence strategy that credibly signals the level and type of response non-state actors can expect in retaliation for each.

In closing, U.S. deterrent strategy should include more specificity to clarify the correlation between punishment and undesired actions to increase the effectiveness of deterrence. An attack-based retaliation strategy would provide that specificity by clearly articulating the credible costs to be imposed on the nodes-of-influence for committing an attack. Coincidently, evaluations of the expected retaliation for cyber and nuclear terrorism scenarios of this study provide the components to develop an example of an attack-based retaliation framework, which is illustrated in Table 5. The first column lists the targets that were validated in Chapter II as relevant centers of gravity for influencing non-state actors' decisions. The subsequent columns list credible threats for retaliating against those targets by type of attack. The retaliatory threats in each box meet the

criteria of a plausible response for the particular type of attack while targeting an appropriate vulnerability for deterring terrorism. For example, attacking the terrorist network was validated as a relevant target for retaliation. Tracing across the table to the cyber terrorism column yields the credible threats of retaliation for a cyber attack: capture and prosecute terrorist members, sever the links between leaders and cells, and restrict travel of all known associates. In contrast, the threat of retaliation for a nuclear attack would be a more aggressive kill or capture campaign that involves military operations and clandestine methods to hunt down the entire terrorist network. Obviously, the example framework depicted in Table 5 is not meant to serve as a policy ready strategy, but merely to provide a methodological approach that would increase the potential impact of punitive deterrence in U.S. counterterrorism efforts.

Retaliation Framework for U.S. Deterrence Policy (Example)		
Targets of Retaliation (Unchanged)	**Cyber Terrorism (Sample Threats)**	**Nuclear Terrorism (Sample Threats)**
Ideology	Information operations campaign	Information operations campaign, democratization
Terrorist network	Capture terrorists, sever links, restrict travel	Kill or capture
Finances	Seize assets, shutdown charities, seek financial reparations	Seize assets, shutdown charities, seek financial reparations
Communications	Disrupt communication capabilities and Internet access	Disrupt communication capabilities and Internet access
Weapons and materiel	Target terrorist cyber-networks and electronic hardware	Destroy residual capabilities and target criminal elements
State sponsor	Cyber warfare on host nation's network	Economic sanctions, regime change, reparations, and conventional military war
Safe havens	Military strikes on terrorist facilities	Military strikes, economic sanctions, host nation regime change
Nuclear retaliation	None	Specifically declare as response against a state that willingly sponsored nuclear terrorism

Table 5. Proposed attack-based retaliation framework for U.S. deterrence policy

C. LEVERAGING DETERRENCE

The counterterrorism methods found in recent policy were developed to support an offensive campaign against terrorism and an associated doctrine of prevention and preemption, and have not been emphasized as part of an effort to send a deterrence message aimed at those non-state organizations yet to commit terrorist attacks on the United States. However, many counterterrorism objectives are difficult to accomplish in the prevention stage, yet become much easier to enforce in the punishment stage. For example, consider the difficulty of policing charity organizations on a global scale until after an attack when investigators are able to narrow the search parameters to effectively trace funding channels. "One reason that the global charitable sector remains vulnerable to terrorist financing is that charities are still subjected to lesser regulatory requirements."[142] However, post-9/11 efforts to combat Al Qaeda financing have been effective. For example, "in his July 2005 letter to Abu Musab al-Zarqawi, Ayman al-Zawahiri humbly asked the leader of al Qaeda in Iraq if he could spare a payment of approximately one hundred thousand because many of the lines have been cut off."[143]

Since several aspects of these counter-terrorism methods occur outside the continental United States, gaining international cooperation would be advantageous. In order to provide for a meaningful and lasting campaign, members of the global community must take action to establish cooperative agreements for freezing terrorists' financial assets and seizing those funds to use for financing future counter-terrorism operations. Additionally, laws must be established in all nations to prosecute those practicing cyber-warfare as telecommunications transcend national borders. The international community must be able to collectively pursue terrorist suspects across borders and bring them to justice.

---

[142] Levitt and Jacobson, "The U.S. Campaign to Squeeze Terrorists' Financing," 67–85, 78.

[143] Ibid., 79.

D. AREAS FOR FURTHER RESEARCH

This study touched upon several areas that provide opportunities for further study and debate. First, while this thesis attempted to show the value and purpose of an attack-based retaliation framework, additional research and analysis would have to be accomplished before this approach could be realized in U.S. deterrence strategy. Those efforts would need to determine what forms of terrorism the United States intends to deter in order to develop a complete list of attack scenarios. Then, potential retaliation options would need to be evaluated as responses to each of those scenarios to flesh out an operational retaliation framework.

The second area that requires additional research relates to the application of "extended deterrence" in deterring terrorist attacks. Assuming the United States developed a more defined retaliation policy for deterring terrorist attacks, should the United States guarantee that response for an attack on its allies as well? Currently, the practice of extended deterrence is crucial to the stability and security of allies in Europe and Asia because it provides a nuclear umbrella that triggers the same response to an attack on them as one on America. Applying this concept to deterring terrorism would obviously pose significant challenges based on the variety and severity of retaliation options, but seems likely that it would at least apply to state-sponsored nuclear terrorism.

Next, an interesting possibility for retaliating against permissive states that were the host nation of a catastrophic cyber attack on the United States is electromagnetic pulse. Detonating a nuclear weapon at high attitudes above the target state, the punisher could generate an electromagnetic pulse to destroy electronics of the host nation. Just as cyber terrorism only inflicts electronic damage on the United States, EMP retaliation would limit destructiveness to electronics of the enemy. However, using a nuclear weapon in response to a non-WMD attack would break the nuclear taboo and raise issues concerning international norms. Also, the actual effects of this application would need to be addressed in order to evaluate the degree of punishment as it relates to the crime. Coincidentally, the discussion on nuclear retaliation exposed an issue not explored in this

study due to its complexity. While the door may not open for nuclear weapons, public tolerance for other measures may relax. For example under less destructive attacks it would be taboo and inconceivable to establish a deterrent message that threatens to destroy historic or religious places— yet it might be more plausible in response to an act of nuclear terror. Further research may provide additional retaliation options that would increase the effectiveness of deterrence for certain attacks.

APPENDIX

A Possible Set of "Realistic" Estimated Results for a 10 kiloton Nuclear Device									
	Numbers of People in Thousands (k)								
	Zone 1 (0.76 km)	**Zone 2** (0.82 km)	**Zone 3** (1.0 km)	**Zone 4** (1.2 km)	**Zone 5** (380 REM)	**Zone 6** (280 REM)	**Zone 7** (210 REM)	**Zone 8** (150 REM)	**Zone 9** (1 REM)
Total Population	14.6	16.9	31.7	46.6	203	236	270	303	439
Total fatalities*	13	17	19	21	82	91	94	97	99
Instant (within minutes)	7.7	8.5	8.6	8.6	8.6	8.6	8.6	8.6	8.6
Within 24 hours	9.8	11	13	15	45	45	45	45	45
Within 96 hours	10	13	15	16	61	62	62	62	62
Within 8 weeks	11	14	15	17	66	71	79	83	85
Injuries (initially alive)**	4.1	7.9	9.1	18.7	**106**	**123**	**128**	**136**	**138**
Blunt trauma plus other effects	.6	.9	1.0	1.1	1.1	1.1	1.1	1.1	1.1
Burns	.8	1.4	1.6	1.7	1.7	1.7	1.7	1.7	1.7
Prompt radiation	.5	.6	.7	.7	.7	.7	.7	.7	.7
Multiple (excluding fallout)	2.3	2.6	2.9	3.2	3.2	3.2	3.2	3.2	3.2
Able to walk	1.5	4	7	15	101	123	128	136	138
Requiring special care	3.9	7.5	8.5	17	80	84	89	91	95
Injuries from Fallout	.1	.3	3.6	12	99	116	121	129	131
Eye Damage***									
Flash Blindness	.2	.7	1.6	1.8	2.2	2.3	2.4	2.4	2.5
Retinal Burns	.1	.3	.5	.7	.9	.9	1.0	1.0	1.1
Evacuation needed****	6.9	8.4	23.1	38	**194**	**227**	**261**	**294**	**430**
Critical to evacuate	Extreme?	Extreme?	Extreme	Extreme	Very	Yes	Yes	Yes	Less so
Needing shelter	6.9	8.3	17	28	150	170	200	225	310
Requiring decontamination	6.9	8	20	32	75	82	91	101	110
Major fires (not in thousands)*****	200	220	235	245	247	250	250	250	250
Infrastructure									
Electrical Power									
Out for more than 1 week	Yes	Yes	Yes	Yes	Yes	Likely	Maybe	Maybe	Maybe
Out for more than 4 weeks	Yes	Yes	Yes	Likely	Maybe	No	No	No	No
City Water System									
Contamination with radiation	Unlikely	No	No	No	No	No	No	No	No
Contaminated with "dirt"	Yes	Maybe	No	No	No	No	No	No	No
Telecommunication									
Out for more than 1 week	Yes	Yes	Yes	Yes	Yes	Yes	Likely	Likely	Likely
Out for more than 4 weeks	Yes	Yes	Yes	Yes	Likely	Maybe	Maybe	No	No
EMP damage	Yes	Yes	Likely	Maybe	No	No	No	No	No
This table indicates a **possible** set of consequences for people in a given zone at the time of the detonation. The numbers are accumulative with respect to the zones (e.g., Zone 2 includes the values for Zone 1). **Note that these results depend strongly on the assumptions used and the methods used to apply those assumptions. The values are estimates and are not supported by computer calculations.**									

Table 6. A possible set of realistic estimated results from individuals in a given zone at the time of detonation of a 10 kiloton nuclear device. (From 2005 National Planning Scenarios page 1–39.)[144]

[144]United States Department of Homeland Security, *National Planning Scenarios*, 1.39.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allison, Graham T. and Morton H. Halperin. 2007. "Bureaucratic Politics: A Paradigm and some Policy Implications." *World Politics*, no. 24 , Supplement: Theory and Policy in International Relations (Spring, 1972): 40–79, http://www.jstor.org/stable/2010559 (accessed 7/14/2009).

Auerswald, David P. 2006. "Deterring Nonstate WMD Attacks." *Political Science Quarterly* 121, 4:543–568.

Berman, E. 2003. "Hamas, Taliban and the Jewish Underground: An Economist's View of Radical Religious Militias." *SSRN Working Paper Series* (Oct, 2003).

Blanchard, Christopher M. 2006. *Al Qaeda: Statements and Evolving Ideology*. Ft. Belvoir: Defense Technical Information Center, www.dtic.mil (accessed 8/10/2009).

Bowen, Wyn. 2004. "Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism." *Contemporary Security Policy* 25, 1:54–70.

Brimley, Shawn. 2006. "Tentacles of Jihad: Targeting Transnational Support Networks." *Parameters: Journal of the US Army War College* 36, 2:30–46, www.dtic.mil (accessed 7/18/2009).

Cimbala, Stephen J. 2001. *Deterrence and Nuclear Proliferation in the Twenty-First Century*. Westport, CN.: Praeger.

Colby, Elbridge A. 2007. "Restoring Deterrence." *Orbis* 51, 3:413–428.

———. 2008. "Expanded Deterrence: Broadening the Threat of Retaliation." *Policy Review* 149:43–59.

Corr, Anders. 2005. "Deterrence of Nuclear Terror." *The Nonproliferation Review* 12, 1: 127–147, http://www.informaworld.com/10.1080/10736700500208876 (accessed 4/21/2009).

Davis, Paul K. and Brian M. Jenkins. 2002. *Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda*. Santa Monica, CA: Rand, http://www.rand.org/publications/MR/MR1619/ (accessed 4/15/2009).

Dunn, Lewis A. 2001. "Rethinking Deterrence: A New Logic to Meet Twenty First Century Challenges." Chapter 2, In *Deterrence and Nuclear Proliferation in the Twenty-First Century*, edited by Stephen J. Cimbala, 23–38. Westport, CN.: Praeger.

Executive Office of the President. 2006. *The National Security Strategy of the United States of America*. Washington, DC: The White House.

———. 2006. *National Strategy for Combating Terrorism*. Washington, D.C.: The White House.

———. 2003. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assests*. Washington, D.C.: The White House.

———. 2002. *National Strategy to Combat Weapons of Mass Destruction*. Washington, D.C: The White House.

Fearon, James D. 1995. "Rationalist Explanations for War." *International Organization* 49, 3:379–414.

Freedman, Lawrence. 2004. *Deterrence*. Cambridge, UK; Malden, MA: Polity Press.

———. 2003. *The Evolution of Nuclear Strategy*. 3rd ed. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.

Gartenstein Ross, Daveed, Joshua D. Goodman, and Laura Grossman. 2009. *Terrorism in the West 2008 a Guide to Terrorism Events and Landmark Cases*. Washington, DC: FDD's Center for Terrorism Research, http://www.hsdl.org/ (accessed 8/10/2009).

George, Alexander L. 2003. "The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries." Chap. 10, In *Know Thy Enemy: Profiles of Adversary Leaders and their Strategic Cultures*, edited by Barry R. Schneider and Jerrold M. Post. 2nd ed., 325. Maxwell Air Force Base, AL.; Wash. D.C.: USAF Counterproliferation Center.

Gorman, Siobahn. 2009. "China Expands Cyberspying in U.S., Report Says." *Wall Street Journal*, October 23, , sec. Technology, http://online.wsj.com/article/SB125616872684400273.html?mod=WSJ_hpp_MIDDLTopStories (accessed 10/23/2009).

Hart, Paul't. "Irving L. Janis' Victims of Groupthink." 1991. *Political Psychology* 12, 2:247–278.

Herren, Eric. 2009. "Counter-Terrorism Dilemmas." International Institute for Counter-Terrorism, http://www.ict.org.il/articles/ (accessed 6/1/2009).

House International Relations Committee. 2005. *Does our Counter-Terrorism Strategy Match the Threat?* CT-250 sess., 09/29/2005, www.dtic.mil (accessed 7/14/2009).

Homeland Security Council. 2007. *National Strategy for Homeland Security*. Washington, D.C.: Executive Office of the President.

Kapur, S. Paul. 2009. "Deterring Nuclear Terrorists." In *Complex Deterrence: Strategy in the Global Age*, edited by T. V. Paul, Patrick M. Morgan and James J. Wirtz. Chicago; London: The University of Chicago Press.

Kean Commission. 2008. "9/11 Intelligence Failure." Chap. 32, In *Intelligence and National Security: The Secret World of Spies: An Anthology*, edited by Loch K. Johnson and James J. Wirtz. 2nd ed., 417–458. New York: Oxford University Press.

Knopf, Jeffrey W. 2008. "Wrestling with Deterrence: Bush Administration Strategy after 9/11." *Contemporary Security Policy* 29, 2:229–265.

———. N.D. "The Fourth Wave in Deterrence Research." *Forthcoming in Contemporary Security Policy*.

Kohn, Bryan S. 2002. *Attacking Islamic Terrorism's Strategic Center of Gravity*. Ft. Belvoir: Defense Technical Information Center, www.dtic.mil (accessed 7/14/2009).

Lebow, Richard Ned and Janice Gross Stein. 1989. "Rational Deterrence Theory: I Think, therefore I Deter." *World Politics* 41, 2:208–224.

Levitt, Matthew and Michael Jacobson. 2008. "The U.S. Campaign to Squeeze Terrorists' Financing." *Journal of International Affairs* 62, 1:67–85.

Lewis, T. G. 2006. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, N.J.: Wiley-Interscience.

Lynch, Colum. 2002. "War on Al Qaeda Funds Stalled. Network 'Fit and Well,' Ready to Strike, Draft of UN Report Says." *Washington Post*, August 29, 2002, sec. A, http://www.highbeam.com/doc/1P2-382734.html (accessed 08/10/2009).

Melese, Francois and Diana Angelis. 2004. "Deterring Terrorists from using WMD: A Brinkmanship Strategy for the United Nations." *Defense & Security Analysis* 20, 4:337–341.

Merari, Ariel. 2002. "Deterring Fear: Government Responses to Terrorist Attacks." *Harvard International Review* 23, 4:26–31.

Miller, Michael. 2007. "Nuclear Attribution as Deterrence." *Nonproliferation Review* 14, 1:33–60.

Perl, Raphael F. 2007. *National Strategy for Combating Terrorism: Background and Issues for Congress*. Ft. Belvoir: Defense Technical Information Center, http://handle.dtic.mil/100.2/ADA473792. (accessed 8/26/2009).

Perry, William J., Charles D. Ferguson, and Brent Scowcroft. 2009. *U.S. Nuclear Weapons Policy*. Council on Foreign Relations, http://www.cfr.org/content/publications/attachments/Nuclear _Weapons_TFR62.pdf. (accessed September 10, 2009).

Rabasa, Angel, Peter Chalk, Kim Cragin, Sara A. Daly, Heather S. Gregg, Theodore W. Karasik, Kevin A. O'Brien, and William Rosenau. 2006, *Beyond Al-Qaeda. Part 1. the Global Jihadist Movement*. Santa Monica, CA: RAND Corporation, www.dtic.mil (accessed 7/14/2009).

Report by the National War College Student Task Force on Combating Terrorism. 2002. *Combating Terrorism in a Globalized World* . Washington, D.C.: National War College, www.au.af.mil/au/awc/awcgate/ndu/n02combating_terrorism.pdf (accessed 10/18/2009).

Schelling, Thomas C. 1966. *Arms and Influence*. New Haven, CT: Yale University Press.

Schneider, R. and Jerrold M. Post, eds. 2003. *Know Thy Enemy: Profiles of Adversary Leaders and their Strategic Cultures*. 2nd ed. Maxwell Air Force Base, Ala.: USAF Counterproliferation Center, Air War College, Air University.

Schwartz, Stephen I. 1998. *Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons since 1940*. Washington, D.C.: Brookings Institution Press.

Servold, Gary M. 2003. "The Muslim Brotherhood and Islamic Radicalism." Chap. 10, In *Know Thy Enemy: Profiles of Adversary Leaders and Their Strategic Cultures*, edited by Barry R. Schneider and Jerrold M. Post. 2nd ed., 41. Maxwell Air Force Base, Ala.; Wash. D.C.: USAF Counterproliferation Center.

Steinberg, Gerald M. 2001. "Rediscovering Deterrence after September 11, 2001." *Jerusalem Letter/Viewpoints* No. 467, http://www.jcpa.org/jl/vp467.htm (accessed 4/10/2008).

Sunzi and J. H. Huang. 1993. *Sun Tzu: The New Translation* [Sunzi bing fa.]. 1st ed. New York: Quill.

Trager, Robert F. and Dessislava P. Zagorcheva. 2005. "Deterring Terrorism: It can be done." *International Security* 30, 3:87–123.

United States Department of Homeland Security. 2005. *National Planning Scenarios*. Washington D.C.: United States Department of Homeland Security, http://www.ccroa.org/index.php (accessed 8/08/2009).

———. 2004. *National Planning Scenarios: Executive Summary*. Washington D.C.: United States Department of Homeland Security, http://www.ccroa.org/index.php (accessed 8/08/2009).

———. 2003. *The National Strategy to Secure Cyberspace*. Washington, D.C.: United States Department of Homeland Security.

Whiteneck, Daniel. 2005. “Deterring Terrorists: Thoughts on a Framework.” *The Washington Quarterly* 28, 3:187–199.

Younger, Stephen Michael. 2009. *The Bomb: A New History*. 1st ed. New York: Ecco Press.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California